ΠME Journal, Vol. xx, No. x, pp 373–??, xxxx.

THE PI MU EPSILON 100TH ANNIVERSARY PROBLEMS: PART I

STEVEN J. MILLER*, JAMES M. ANDREWS†, AND AVERY T. CARR‡

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!

1914

Martin Gardner

Few twentieth-century mathematical authors have written on such diverse subjects as Martin Gardner (1914–2010), whose books, numbering over seventy, cover not only numerous fields of mathematics but also literature, philosophy, pseudoscience, religion, and magic. Today, he is best known as a recreational mathematician, a term that reflects perhaps not the branches of mathematics he favored but the accessible manner in which he presented them. As Gardner wrote in the introduction to his first book of puzzles, *Hexaflexagons, Probability Paradoxes, and the Tower of Hanoi*,

> There is not much difference between the delight a novice experiences in cracking a clever brain teaser and the delight a mathematician experiences in mastering a more advanced problem. Both look on beauty bare—that clean, sharply defined, mysterious, entrancing order that underlies all structure.

A philosophy major at the University of Chicago, Gardner worked as a reporter, yeoman in the Navy, and writer for a children's magazine before writing his first article for *Scientific American* in 1956. The publisher enjoyed the article and asked Gardner to turn it into a monthly puzzle column, which would run for over twenty-five years and spawn fifteen books, reaching and inspiring countless mathematical hobbyists.

Centennial Problem 1914. *Proposed by Byron Perpetua, Williams College.*

The following problem is classic Gardner: easily stated and solvable without advanced techniques, yet challenging and surprising. Take a solid sphere and drill a cylindrical hole 6 inches long through its center (this means that the height of the cylinder is 6 inches; the caps on the bottom and top, which are removed from the

*Williams College, Senior Editor
†University of Memphis, Editor
‡Emporia State University, Editor

sphere when we drill our hole, are not counted). What is the sphere's remaining volume? One approach is straightforward but slow; the other is clever and skips several computations. *Hint:* although the problem seems to be missing necessary information, it likely wouldn't be posed unless it had a unique solution. While it requires some effort to prove that all possible realizations lead to the same answer, there is a particularly simple case which you can compute easily.

REFERENCES

[1] M. Gardner, "Hexaflexagons, Probability Paradoxes, and the Tower of Hanoi", Cambridge, New York, 2008.

[2] E. Peres, "Martin Gardner: The Mathematical Jester", *Mathematical Lives: Protagonists of the Twentieth Century from Hilbert to Wiles*, ed. Claudio Bartocci et al., Springer-Verlag, Berlin, 2011.

[3] J. J. O'Connor and E. F. Robertson, "Martin Gardner", MacTutor History of Mathematics. http://www-history.mcs.st-and.ac.uk/Biographies/Gardner.html.

1918

Georg Cantor: 1845–1918

One of the greatest difficulties in mathematics is handling infinities; the subject is so tricky that there are even some who prefer to never to deal with such matters. The results in the field can be quite surprising. For example, not all infinities are the same size. This is a strange concept, and requires some preliminaries to define properly. We say two sets A and B have the same size (or equivalently are the same cardinality) if there is an invertible, one-to-one and onto function $f : A \to B$; recall one-to-one means distinct inputs are sent to distinct outputs, and onto means every element of B is hit. Such a function allows us to put A and B in a one-to-one correspondence. For example, if A is the set of all positive integers and S is the set of squares of positive integers, both sets are infinite and both have the same number of elements, as we can see by taking the function f to be $f(n) = n^2$. What makes this result strange at first is that while B is a proper subset of A, they can be put into a one-to-one correspondence.

The smallest infinity is the cardinality of the natural numbers, which is equivalent to the cardinality of the integers as well as that of the rationals. Cantor proved in 1874 that there are 'more' irrational numbers than rationals; equivalently, the cardinality of the real numbers is strictly larger than the cardinality of the rationals. He gave a later proof in 1891 where he introduced his diagonalization method, which is now a staple in most analysis courses. An important consequence of these results is that the transcendental numbers have a larger cardinality than the algebraic numbers. Algebraic numbers are roots of polynomials of finite degree with integer coefficients; these include not just the rationals, but numbers such as $2^{1/3}$, $i = \sqrt{-1}$, and $\sqrt{\sqrt{3}+\sqrt{5}}$ (the three polynomials can be taken to be x^3-2, x^2+1 and x^8-16x^4+4). Transcendental numbers are what remains.

Typically it is very hard to prove a given number is transcendental; we know some special numbers such as π (first proved by Lindemann in 1882) and e (due to Hermite in 1873) are. Louiville gave a construction in 1851 that proves certain numbers, such as $\sum_{n=1}^{\infty} 10^{-n!}$, are transcendental. His argument runs as follows. If α is algebraic and is a root of an irreducible polynomial of degree d with integral coefficients, one can show that we cannot approximate α too well by rationals. Specifically, for any C there are only finitely many relatively prime rational numbers p/q such that $|\alpha - p/q| \le C/q^d$. If we could approximate α too well, the only option for it is to be transcendental.

Centennial Problem 1918. *Proposed by Steven J. Miller, Williams College.*

Interestingly, Cantor's diagonal method is an existential one, not a constructive one. It proves there are far more transcendentals than algebraic numbers, but it does not actually construct one. Modify Liouville's construction to create uncountably many transcendental numbers. In particular, find a one-to-one function $f : [0,1] \to [0,1]$ such that $f(x)$ is always transcendental. Can you find a continuous function that does this? If yes, can you make your function differentiable?

As an aside, a natural additional question to ask concerns the distribution of the sizes of the different infinities. We've said the rationals (or, it turns out, the algebraic numbers too) are the lowest infinity, while the real numbers are a higher one. Are there any sets of cardinality strictly between these two? To find out more about this, look up the Continuum Hypothesis, finally resolved by Paul Cohen in 1963.

REFERENCES

[1] G. Cantor, "Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen", Journal für die Reine und Angewandte Mathematik **77** (1874), 258–262.

[2] G. Cantor, "Über eine elementare Frage der Mannigfaltigskeitslehre", Jahresbericht der Deutschen Mathematiker-Vereinigung **1** (1891), 75–78.

[3] J. J. O'Connor and E. F. Robertson, "Georg Ferdinand Ludwig Philipp Cantor", MacTutor History of Mathematics.
http://www-history.mcs.st-andrews.ac.uk/Biographies/Cantor.html.

[4] S. J. Miller and R. Takloo-Bighash, "An Invitation to Modern Number Theory", Princeton University Press, 2006.

1922

Lindeberg condition

In probability theory a continuous random variable X has density f_X if (1) $f_X(x) \geq 0$, (2) $\int_{-\infty}^{\infty} f_X(x)dx = 1$, and (3) the probability X takes on a value between a and b is the integral of f_X from a to b; this is one of the most important applications of integration, namely that it allows us to find probabilities. One of the most important continuous densities is that of the normal distribution. We say X is normally distributed with mean μ and variance σ^2 if its density is $(2\pi\sigma^2)^{-1/2} \exp\left(-(x-\mu)^2/2\sigma^2\right)$. The more names something has, typically the more important it is; we also call this density a Gaussian, or say its the bell curve.

Given a random variable X let μ_X denote its mean and σ_X its variance. We can standardize X by passing to $(X - \mu_X)/\sigma_X$, which has mean 0 and variance 1. As its name suggests, one of the most important theorems in the subject is the Central Limit Theorem. This says that for appropriate random variables X_i, as $n \to \infty$ if we set $Y_n = X_1 + \cdots + X_n$ then $Z_n := (Y_n - \mu_{Y_n})/\sigma_{Y_n}$ converges to being normally distributed.

The Central Limit Theorem has a long and rich history, with a perennial quest to find the weakest possible conditions. In 1922 Lindeberg proved that a certain set of conditions on the X_i sufficed to ensure convergence to a normal distribution. Specifically, consider the following situation. Let X_k be a random variable on a probability space, and assume the means μ_{X_k} and variances $\sigma_{X_k}^2$ exist and are finite. Let $I(|X_k| \geq \epsilon s_n)$ be 1 if $|X_k| \geq \epsilon s_n$ and 0 otherwise, and let $\mathbb{E}[\cdots]$ denote expectation relative to the underlying probability space. If $s_n^2 = \sum_{k=1}^n \sigma_{X_k}^2$ and for all $\epsilon > 0$ we have $\lim_{n\to\infty} \sum_{k=1}^n \mathbb{E}[(X_k - \mu_{X_k})^2 I(X_k) \geq \epsilon s_n)]/s_n^2 = 0$ then Z_n converges to a Gaussian. If we additionally assume $\max_k \sigma_{X_k}^2/s_n^2 \to 0$ then this condition is also necessary.

Centennial Problem 1922. *Proposed by Steven J. Miller, Williams College.*

Consider the following twist. Imagine that instead of caring about the sum $X_1 +$

$\cdots + X_n$, we now only care about its value modulo 1; this means we look at its value and subtract the greatest integer at most it. This cannot converge to a Gaussian as it is only nonzero in an interval of length 1. What do you expect this sum to converge to? What is the most general set of conditions required to ensure such convergence? This problem is an important tool for understanding products of random variables, as the distribution of a product is the sum of the logarithms. One particularly important application is in Benford's law (see the problem from 1938 or [**?**]).

REFERENCES

[1] J. W. Lindeberg, "Eine neue Herleitung des Exponentialgesetzes in der Wahrscheinlichkeitsrechnung", Mathematische Zeitschrift **15** (1922) (1), 211–225.

[2] S. J. Miller and M. Nigrini, "The Modulo 1 Central Limit Theorem and Benford's Law for Products", International Journal of Algebra **2** (2008), no. 3, 119–130. http://arxiv.org/pdf/math/0607686v2.

1926

Ackermann's Function

In 1926 David Hilbert published an article on infinity, at that time still a somewhat controversial topic in mathematical philosophy, in which he famously declared, "No one will drive us from the paradise which Cantor created for us." In this important paper, Hilbert described a function discovered by his student Wilhelm Ackermann. Ackermann was trying to unify arithmetic operations on natural numbers. Just as, in some sense, addition is repeated counting, multiplication is repeated addition, and exponentiation is repeated multiplication, one can continue to iterate each successive operation to produce an even faster-growing one. Ackermann defined his function φ of three variables recursively in such a way that $\varphi(a,b,0) = a+b$, $\varphi(a,b,1) = a \cdot b$, $\varphi(a,b,2) = a^b$, $\varphi(a,b,3) = a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}$ with b a's in the exponent, and so on. The significance from a mathematical point of view, explained in Ackermann's subsequent paper, is that this function is computable (the technical term is *recursive*) but only by using dirty tricks like double recursion, unbounded loops, or the operator "the least n such that." (Functions that can be computed in a more straightforward manner, without resort to such devices, are called *primitive recursive*.) The theory of computability has grown to be a major branch of mathematical logic and theoretical computer science; there are about 5000 papers in MathSciNet under the primary classification 03D (Computability and Recursion Theory). Obviously φ grows astronomically as its arguments increase. Other authors later simplified the definition but kept the spirit. The cleanest version is due to Raphael Robinson:

$$A(i,j) \;=\; \begin{cases} j+1 & \text{if } i = 0 \\ A(i-1,1) & \text{if } i > 0 \text{ and } j = 0 \\ A(i-1, A(i, j-1)) & \text{if } i > 0 \text{ and } j > 0. \end{cases}$$

To get an idea of how fast the function grows, note that $A(2,3) = 9$, $A(3,3) = 61$, and $A(4,3)$ has about 10^{20000} decimal digits. One cannot begin to comprehend the enormity of $A(5,3)$.

Because Ackermann's function (in whatever variation) grows very rapidly, one can form a kind of "inverse" function, α, of one variable, which grows so slowly that for all practical purposes it is constant. This function turns out to play a role in the analysis of algorithms. For example, although there is no linear-time algorithm for managing a sequence of "union" and "find" operations on a collection n disjoint sets, Robert Tarjan found a data structure such that these operations can be performed in time $O(n \cdot \alpha(n))$.

Centennial Problem 1926. *Proposed by Jerrold Grossman, Oakland University.*

Here is a problem about a modification (pun intended) of the Ackermann function. Let $\mathbf{N}$ denote the set $\{0, 1, 2, 3, \ldots\}$ of natural numbers, and for each integer $n > 2$ let $\mathbf{N}_n$ denote the set $\{0, 1, 2, \ldots, n-1\}$ of natural numbers less than n. Define a function A_n from $\mathbf{N} \times \mathbf{N}_n$ to $\mathbf{N}_n$ as follows:

$$A_n(i,j) \;=\; \begin{cases} j+1 \bmod n & \text{if } i = 0 \\ A_n(i-1, 1) & \text{if } i > 0 \text{ and } j = 0 \\ A_n(i-1, A_n(i, j-1)) & \text{if } i > 0 \text{ and } j > 0. \end{cases}$$

If you play around with this function for various small values of n (make a table of its values for small i and j), you will find that $A_n(i,j)$ quickly becomes constant. For example, $A_{13}(i,j) = 9$ for all j once $i \geq 6$. Prove or disprove that this behavior happens for all n.

REFERENCES

[1] W. Ackermann, "Zum Hilbertschen Aufbau der reellen Zahlen", Math. Ann. **99** (1928), 118–133. http://eretrandre.org/rb/files/Ackermann1928_126.pdf.

[2] D. Hilbert, "Über das Unendliche", Math. Ann. **95** (1926), 161–190.

[3] R. M. Robinson, "Recursion and double recursion", Bull. Amer. Math. Soc. **54** (1948), 987–993. http://www.math.ntnu.no/emner/MA2301/2010h/robinson_doublerec.pdf.

[4] R. E. Tarjan, "Efficiency of a good but not linear set union algorithm", J. Assoc. Comp. Mach. **22** (1975), 215–225. http://ecommons.library.cornell.edu/handle/1813/5942.

1930

Ramsey Theory

"Suppose aliens invade the earth and threaten to obliterate it in a year's time unless human beings can find the Ramsey number for red five and blue five. We could marshal the world's best minds and fastest computers, and within a year we could probably calculate the value. If the aliens demanded the Ramsey number for red six and blue six, however, we would have no choice but to launch a preemptive attack." Paul Erdős.

There are many questions where we can easily set up a calculation to determine the answer, but not only currently lack the computational power to perform it, but will lack the power for many years to come. A great source of such problems is Ramsey Theory. Probably the most famous of these problems is the determination of the Ramsey number $R(m,n)$, which is defined as follows. Imagine there is a party with N people, and in any pair of two people either both know each other, or neither knows the other. Then $R(m,n)$ is the smallest N such that, no matter whom knows whom, there are either at least m people that all know each other, or there are at least n people such that none of these n know anyone else in this set of n. Some authors use like and dislike instead of know and don't know. A nice calculation gives $R(3,3) = 6$ (and $R(4,4) = 18$); Erdős' quote is about $R(5,5)$ (which we know lies between 43 and 49) and $R(6,6)$ (which is between 102 and 165). Ramsey Theory's mantra is "Complete Disorder Is Impossible;" given any large structure inside it lies a small substructure which has strong structure. Unfortunately, there are often so many cases to investigate that these problems cannot be solved by brute force attacks. For example, we may associate a graph to the party problem, with the people as vertices and connecting two people who know each other with an edge. The number of possible graphs on N labeled vertices is $2^{\binom{n}{2}} = 2^{n(n-1)/2}$, which already exceeds 10^{200} for $n = 40$!

Centennial Problem 1930. *Proposed by From the 1953 Putnam Mathematical Examination; text and problem choice by Joel Spencer (NYU), James Andrews, and Steven J. Miller (Williams College):.* Six points are in general position in space (no three on a line, no four in a plane). The fifteen line segments joining them in pairs are drawn and then painted, some segments red, some blue. Prove that some triangle has all its sides the same color.

REFERENCES

[1] A. Carr, "Party at Ramsey's", available online at http://blogs.ams.org/mathgradblog/2013/05/11/mathematics/.

[2] R. L. Graham and J. H. Spencer, "Ramsey Theory", Scientific American (July 1990), p. 112–117. http://www.math.ucsd.edu/~ronspubs/90_06_ramsey_theory.pdf.

[3] F. P. Ramsey, "On a Problem of Formal Logic", Proc. London Math. Soc. (1930), s2-30 (1): 264–286. http://www.cs.umd.edu/~gasarch/TOPICS/ramsey/ramseyorig.pdf.

1934

Khinchin's Constant

Each real irrational number x has a unique *continued fraction* expansion, that is, a representation of the form

$$x \;=\; a_0(x) + \cfrac{1}{a_1(x) + \cfrac{1}{a_2(x) + \cfrac{1}{\ddots}}}$$

where the $a_i(x)$ are called the continued fraction digits of x. A. Y. Khinchin proved the remarkable fact that, for almost every real number x, the geometric mean of the first n digits in the continued fraction expansion of x converges to *the same constant* K as $n \to \infty$ (i.e., $\lim_{n\to\infty} \sqrt[n]{a_1(x)a_2(x)\cdots a_n(x)} = K$ for almost all x). The original proof used only elementary (but messy) measure theory, while modern proofs are based on the mean ergodic theorem. This constant K is known as *Khinchin's constant*, with a numerical value of approximately 2.6854520010. It is not known whether this number is rational, algebraic irrational, or transcendental, nor do we know of a nontrivial example of any number x for which the geometric mean of the $a_i(x)$'s converges to Khinchin's constant K, although numerical experiments have shown π, γ, and Khinchin's constant itself to be likely candidates.

Centennial Problem 1934. *Proposed by Jake Wellens, Caltech.*

A number is transcendental if it is not the root of a polynomial of finite degree with rational coefficients; we know e and π are transcendental, and in fact almost all numbers are transcendental. This problem explores some consequences of the believed transcendence of K. Assume that K is transcendental, and let x be an algebraic irrational of degree 2 (thus there are $b, c \in \mathbb{Q}$ such that $x^2 + bx + c = 0$). Prove that for any such x its geometric mean cannot converge to K. Thus, assuming K is transcendental, we know a bit about the structure of the almost nowhere set of numbers whose geometric mean doesn't converge to Khinchin's constant.

REFERENCES

[1] A. Khintchine, "Metrische Kettenbruchprobleme", Compositio Math. **1** (1934), 361–382. http://archive.numdam.org/ARCHIVE/CM/CM_1935__1_/CM_1935__1__361_0/CM_1935__1__361_0.pdf.

1938

Benford's law

The next time you're in a boring meeting or class, calculate the first N Fibonacci numbers (for as large an N as you can) and see what percentage have a first digit of d for each $d \in \{1, \ldots, 9\}$. While it's natural to guess that all digits are equally likely, the answer is far from that. Almost 30% of these numbers start with a 1, while only about 4.5% begin with a 9; in general, the probability of a first digit of d is $\log_{10} \frac{d+1}{d}$. The Fibonaccis are not an isolated oddity; many mathematical and natural data sets exhibit this bias, which is now known as Benford's law. One of the more interesting applications of it is to detect tax fraud. The reason it is so successful is that people are typically horrible random number generators, not putting in enough of the right patterns. For example, if we toss a fair coin 100 times most people know there should be about 50 heads and 50 tails, but they don't know what the longest run of heads or tails should be, or how many alternations between runs of heads and runs of tails should occur. The same is true in creating fake data entries; people are more likely to spread out the leading digit equally from 1 to 9, or concentrate near 5, in the mistaken belief that this makes the data look more plausible. This is now a vast literature on Benford's law and its applications; it surfaces in accounting, computer science, dynamical systems, economics, finance, geology, medicine, number theory, physics, psychology, statistics, ...

A terrific explanation of Benford's law of digit bias is that there is *no* bias, provided we look at the data the right way. Specifically, a data set $\{x_n\}$ is Benford if and only if $\{y_n := \log_{10} x_n\}$ is equidistributed (or uniformly) distributed modulo 1; this means for any $[a, b] \subset [0, 1]$ we have

$$\lim_{N\to\infty} \frac{\#\{n \le N : \log_{10} x_n \bmod 1 \in [a, b]\}}{N} \;=\; b - a.$$

To see why this is true, note that if $y \equiv y' \bmod 1$ (which means that y and y' differ by an integer), then $10^y = 10^{y'+k} = 10^{y'}10^k$ for some integer k. This immediately implies that 10^y and $10^{y'}$ have the same leading digits, as the only difference between these two numbers is the location of the decimal point. Thus if the sequence $\{y_n\}$ is uniformly distributed modulo 1, the probability $y_n \in [0, \log_{10} 2]$ is just $\log_{10} 2$; however, these are precisely the numbers whose first digit is 1 (as 0 exponentiates to 1 and $\log_{10} 2$ exponentiates to 2), and $\log_{10} 2$ is the Benford probability of a first digit of 1. One of the easiest sequences to show is Benford is $x_n = \alpha^n$ for $\log_{10} \alpha$ irrational, as by Weyl's Theorem $n\beta$ is equidistributed modulo 1 if β is irrational (and thus $y_n = \log_{10} x_n = n \log_{10} \alpha$ is uniformly distributed modulo 1 so long as $\log \alpha$ is irrational).

Centennial Problem 1938. *Proposed by Steven J. Miller, Williams College.*

The sequences $\{2^n\}$ and $\{3^n\}$ are both Benford; what about the sequence $\{2^m3^n\}$? For this sequence, we write the numbers in increasing order; thus it begins 1, 2, 3, 4, 6, 8, 9. More generally, is $\{p^m q^n\}$ Benford for p and q disjoint primes?

REFERENCES

[1] F. Benford, "The Law of Anomalous Numbers", Proceedings of the American Philosophical Society **78** (1938), 551–572. http://www.jstor.org/discover/10.2307/984802?uid=3739552&uid=2&uid=4&uid=3739256&sid=21103164625091.

[2] S. J. Miller, ed., "The Theory and Applications of Benford's Law", Princeton University Press, to appear.

[3] R. A. Raimi, "The first digit problem", Amer. Math. Monthly **83** (1976), no. 7, 521–538.

1942

Zeros of $\zeta(s)$

One of the most important functions in number theory is the Riemann zeta function, $\zeta(s)$. Initially defined for $\text{Re}(s) > 1$ by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, using the Fundamental Theorem of Arithmetic (which states every integer can be written uniquely as a product of prime powers) we see that this sum also equals $\prod_{p \text{ prime}}(1-p^{-s})^{-1}$. This relation highlights the central role it plays in studying the primes. The integers are extremely well understood; there are no mysteries left in their distribution! The product relation above connects the integers to the primes, and allows us to pass from knowledge of the integers to knowledge of the primes. For example, the divergence of $\sum_{n=1}^{\infty} 1/n$ implies the infinitude of primes, as does the fact that $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$ (if there were only finitely many primes, the product would be rational at $s = 2$, implying that π^2 is rational, which is false).

Though others had studied this function first, it is named after Riemann because of his seminal investigations in 1859. He related the distribution of zeros of $\zeta(s)$ (or more precisely its meromorphic continuation to the entire complex plane to a function differentiable everywhere except at $s = 1$, where it has a simple pole of residue 1) to estimates on the number of primes at most x, which we denote by $\pi(x)$. One quickly shows this continuation satisfies a functional equation, relating its values at s to those at $1-s$. A little work shows this extended function vanishes only at the negative even integers (these are called the trivial zeros), and at countable many points whose real part is strictly between 0 and 1 (these are called the non-trivial zeros). It is the location of the non-trivial zeros that govern the main terms in our error estimations of the number of primes $\pi(x)$. The Riemann Hypothesis, one of the seven Clay Millennial Problems, asserts that the non-trivial zeros all have real part equal to 1/2. Up to some logarithms, if $\text{Li}(x) = \int_2^x dt/\log t$ then if the largest real part of a zero of $\zeta(s)$ is θ then $|\pi(x) - \text{Li}(x)|$ is essentially of size x^θ. As a non-trivial zero at ρ implies $1-\rho$ is also a zero, we see the error is as small as possible if the Riemann Hypothesis is true. This error being small has enormous consequences throughout mathematics and its applications (especially in cryptography).

Hardy (in 1914) was the first to prove there are infinitely many zeros on the critical line $\text{Re}(s) = 1/2$, though he was not able to prove a positive percentage lie on the line. That changed in 1942, when Selberg showed a small, but positive, percentage of zeros of $\zeta(s)$ are on the critical line. A major advance came in 1974 with the work of Levinson, who proved more than a third of these zeros are on the line. The best results today are around 40%; there is still a long way to go!

Centennial Problem 1942. *Proposed by Steven J. Miller, Williams College.*

What is wrong with the following "proof" that the Riemann zeta function does not vanish if $\text{Re}(s) > 1/2$? We start with the result that there is an analytic continuation for $\zeta(s)$, and if $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ then $\xi(s) = \xi(1-s)$. *Warning: the proposer does not believe this is a proof, nor does he believe this argument can be salvaged!*

1. For each prime p let $h_p(s) = (1-p^{-2s})^{-1}/(1-p^{-s})^{-1}$. Note $h_p(s)$ is never zero or infinity for $\text{Re}(s) > 0$.
2. Let $\zeta_2(s) := h_2(s)\zeta(s)$. The analytic continuation of $\zeta_2(s)$ is simply $h_2(s)$ times the analytic continuation of $\zeta(s)$. Further, $\zeta_2(s)$ and $\zeta(s)$ have the

same zeros for $\mathrm{Re}(s) > 0$. Note

$$\zeta_2(s) \;=\; \left(1-2^{-2s}\right)^{-1} \prod_{p \geq 3} \left(1-p^{-s}\right)^{-1}.$$

3. Similarly set $\zeta_3(s) = h_3(s)\zeta_2(s)$, and observe in our region $\zeta_3(s)$ and $\zeta_2(s)$ (and hence also $\zeta(s)$) have the same zeros. Note

$$\zeta_3(s) \;=\; \left(1-2^{-2s}\right)^{-1} \left(1-3^{-2s}\right)^{-1} \prod_{p \geq 5} \left(1-p^{-s}\right)^{-1}.$$

4. We continue this process, working initially in the region $\mathrm{Re}(s) > 2$ so that everything converges uniformly. We let $\zeta_\infty(s)$ be the limit of $\zeta_p(s)$ as $p \to \infty$. Note this limit exists when $\mathrm{Re}(s) > 2$, and equals $\zeta(2s)$.
5. As $\zeta(2s)$ has an analytic continuation which doesn't vanish for $\mathrm{Re}(s) > 1/2$ (since $\zeta(s)$ does not vanish if $\mathrm{Re}(s) > 1$), each $\zeta_p(s)$ also does not vanish for $\mathrm{Re}(s) > 1/2$. As all these functions have the same zeros in this region, none of them vanish for $\mathrm{Re}(s) > 1/2$. Thus $\zeta(s)$ does not vanish in this region, and hence the Riemann Hypothesis is true.

REFERENCES

[1] E. Bombieri, "The Riemann Hypothesis", Official Clay Problem Description, http://www.claymath.org/millennium/Riemann_Hypothesis/.
[2] H. M. Edwards, "Riemann's Zeta Function", Academic Press, New York, 1974.
[3] G. H. Hardy, "Sur les zéros de la fonction $\zeta(s)$", Comp. Rend. Acad. Sci. **158** (1914), 1012–1014.
[4] N. Levinson, "More than one-third of the zeros of Riemann's zeta function are on $\sigma = 1/2$", Adv. In Math. **13** (1974), no. 4, 383–436.
[5] G. F. B. Riemann, "Über die Anzahl der Primzahlen unter einer gegebenen Grösse", Monatsber. Königl. Preuss. Akad. Wiss. Berlin, Nov. 1859, 671–680 (see Edwards above for an English translation). http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/EZeta.pdf.
[6] A. Selberg, *Contributions to the theory of the Riemann zeta-function*, Arch. Math. Naturvid. **48** (1946), no. 5, 89–155.

1946

Monte Carlo Method

While today it is hard to gaze around a room without seeing a computer, from a smart phone to a thermostat to keyreaders on hotel doors, the situation was very different during WWII. Computers were in their infancy, and were rare, expensive and big. Early computers could fill an entire room, and had enormous power demands. A major leap in their usefulness came when people realized that they could be used for far more than computing exact answers to specific problems by going through the algebra, but additionally could approximate the answers to difficult problems through extensive simulations. This led to what is now called the Monte Carlo method. The quote below is from the excellent history piece [1] (and in 2013 led off the 'history' section of the Wikipedia article [4]).

> *The first thoughts and attempts I made to practice [the Monte Carlo method] were suggested by a question which occurred to me in 1946 as I was convalescing from an illness and playing solitaires. The question was what are the chances that a Canfield solitaire laid out with 52 cards will come out successfully? After spending a lot of time trying to estimate them by pure combinatorial calculations, I wondered whether a more practical method than "abstract thinking" might not be to lay it out say one hundred times and count the number*

> *of successful plays. This was already possible to envisage with the beginning of the new era of fast computers, and I immediately thought of problems of neutron diffusion and other questions of mathematical physics, and more generally how to change processes described by certain differential equations into an equivalent form interpretable as a succession of random operations.*

Monte Carlo techniques are now used to approximate the solution to numerous problems. Rather than finding exact answers, we can frequently simulate millions, or billions, of cases and use that to glean with high probability an excellent approximation to the true answer. An early application was to nuclear reactions, where scientists would approximate both the trajectories of neutrons and the numbers released in each collision. A closer to home example is integration, which not surprisingly goes by the name of Monte Carlo integration. One of the biggest misconceptions about mathematics comes from Calc I and II. There students learn how to find areas by integrating, and flushed with success after success leave thinking integration isn't that much worse than differentiation. Nothing could be further from the truth. Teachers have to work very hard to find functions that have nice anti-derivatives; a general function won't have a closed-form expression for its integral.

For example, imagine we want to find the volume of a region $\mathcal{R}$ in n-dimensional space (this is extremely important in finance, where we might be trying to figure out the value of a loan over several periods). For simplicity assume $\mathcal{R}$ lives inside the n-dimensional unit box $[0,1]^n$, and assume that it is easy to tell if a point is in the region or not. Then all we have to do is uniformly choose N points in the box $[0,1]^n$, and whatever fraction lies in $\mathcal{R}$ is our approximation to its volume. The Central Limit Theorem not only assures us that this is a good approximation, for large N it gives us bounds on the size of the error. For a concrete example, imagine $f(x) = \sin(\pi \sin(\pi x))$ for $0 \leq x \leq 1$; it's very easy to tell if a point $(a,b) \in [0,1]^2$ lies above the x-axis and below the curve $y = f(x)$, but we have no simple, closed-form expression for the anti-derivative of f.

Centennial Problem 1946. *Proposed by Steven J. Miller, Williams College.*

One of the most important steps in the Monte Carlo method is the ability to choose numbers randomly. If you haven't thought about how hard it is to do something truly random, you may be surprised at how hard it is to truly generate a sequence of points uniformly. Frequently one generates a sequence of quasi-random points through a deterministic process, which is often good enough for applications. A popular, early method is the von Neumann middle square digits method, described with some nice references in the 'Random numbers' section of [2]. Given an n digit number, square it to get a $2n$ digit number. Our random number is the middle n digits. We then square that, take the middle n digits of the new product, and obtain our next 'random' number. We continue the process, generating our sequence of numbers. For example, if we start with 4321 our next number is 6710 as $4321^2 = 18671041$, which is then followed by 241.

It's easy to see this process cannot generate numbers uniformly at random, even if we restrict ourselves to numbers from 0 to $10^n - 1$. The reason is simple: this process generates a periodic sequence! In other words, after at most $10^n - 1$ terms we have a repeat, at which point the pattern repeats since all future terms are completely determined from any previous starting value.

This suggests our questions. For each n, what is the shortest period? The longest? How many of the 10^n elements have this shortest (or longest) period? Can you give an example? *Hint: if you can't solve this problem exactly, can you approximate the answer using Monte Carlo techniques?*

REFERENCES

[1] R. Eckhardt, "Stan Ulam, John von Neumann, and the Monte Carlo method", Los Alamos Science, 1987 Special Issue dedicated to Stanislaw Ulam, 131–137. http://library.lanl.gov/cgi-bin/getfile?00326867.pdf.

[2] N. Metropolis, "The beginning of the Monte Carlo method", Los Alamos Science, 1987 Special Issue dedicated to Stanislaw Ulam, 125–130. http://library.lanl.gov/cgi-bin/getfile?00326866.pdf.

[3] N. Metropolis and S. Ulam, "The Monte Carlo Method", Journal of the American Statistical Association **44** (1949), no. 247, 335–341. http://www.jstor.org/stable/2280232.

[4] Wikipedia, "Monte Carlo method". http://en.wikipedia.org/wiki/Monte_Carlo_method.

1950

Arrow's Theorem

Centennial Problem 1950. *Proposed by Michael Jones (possible) .*

REFERENCES

[1] M. Aigner and G. M. Ziegler, "Proofs from The Book ", Springer-Verlag, Berlin, 1998.

1954

Centennial Problem 1954. *Proposed by .*

REFERENCES

[1] M. Aigner and G. M. Ziegler, "Proofs from The Book ", Springer-Verlag, Berlin, 1998.

1958

Smale's paradox

Centennial Problem 1958. *Proposed by .*

REFERENCES

[1] M. Aigner and G. M. Ziegler, "Proofs from The Book ", Springer-Verlag, Berlin, 1998.

1962

The Stable Marriage Problem

Centennial Problem 1962. *Proposed by Paul Kehle (possible).*

REFERENCES

[1] M. Aigner and G. M. Ziegler, "Proofs from The Book ", Springer-Verlag, Berlin, 1998.

1966

Class number one problem

The *class number one* problem is closely related to the theory of binary quadratic forms. A binary quadratic form is a function $f(x,y) = ax^2 + bxy + cy^2$, where a, b, c are integers. Despite their simple appearances, quadratic forms have a rich structure. They have been studied since ancient times, but their modern interest relates to the question of when we expect to find primes of a specific form. Gauss developed much of the theory of quadratic forms in his landmark book *Disquisitiones Arithmeticae*. We recall a few of his definitions. We set $D = b^2 - 4ac$, and call D the *discriminant* of the quadratic form $f(x, y)$. We say an integer m is *represented* by f if there exist coprime integers r, s such that $m = ar^2 + brs + cs^2$. Gauss noticed that for a fixed D, many quadratic forms behave similarly: for example, they represent the same set of integers. Gauss developed a notion of *equivalent* quadratic forms and sorted quadratic forms into equivalence classes. We denote the number of equivalence classes $h(D)$, and call $h(D)$ the *class number* of D. Gauss saw that few discriminants had one equivalence class of quadratic forms, and conjectured he had found all D for which $h(D) = 1$. The quadratic form version of the class number one problem says that $h(D) = 1$ if and only if $D \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$. In 1966, Alan Baker and Harold Stark submitted papers that proved Gauss's class number one conjecture. Their methods were very different, with Baker utilizing the theory of logarithmic forms and Stark studying L-functions and certain Diophantine equations.

Centennial Problem 1966. *Proposed by Kyle Pratt, Bringham Young University.*

Let $D = -28$, so that $h(D) = 1$. Show that $x^2 + 7y^2$ represents infinitely many primes.

REFERENCES

[1] D. Shanks, "On Gauss's Class Number Problems", Mathematics of Computation **23** (1969), no. 105, 151–163.
http://www.ams.org/journals/mcom/1969-23-105/S0025-5718-1969-0262204-1/S0025-5718-1969-0262204-1.pdf.

[2] H. M. Stark, "On complex quadratic fields with class number equal to one", Trans. Amer. Math. Soc. **122** (1966), 112119.
http://www.ams.org/journals/tran/1966-122-01/S0002-9947-1966-0195845-4/S0002-9947-1966-0195845-4.pdf.

[3] H. M. Stark, "A complete determination of the complex quadratic fields of class-number one", Michigan Math. J. 14 1967 127.
http://www.ams.org/leavingmsn?url=http://projecteuclid.org/getRecord?id=euclid.mmj/1028999653.

[4] H. M. Stark, "The Gauss Class-Number Problems", Clay Mathematics Proceedings Volume 7, 2007,
http://www.claymath.org/publications/Gauss_Dirichlet/stark.pdf.

1970

Hilbert's Tenth Problem

One of the most fundamental questions in mathematics is, not surprisingly, also one of the oldest: Given an equation, is there a solution? This is a very general question, and as such there are many issues with our formulation. For example, what kind of equations are we considering? What do we count as a solution? If we're given $x^2 + 1 = 0$ then the two solutions are $i = \sqrt{-1}$ and $-i$; however, neither of these are real numbers and thus some people might object to these being considered roots. Alternatively, consider $r^2 - \pi = 0$. The roots here are $r = \sqrt{\pi}$ and $-\sqrt{\pi}$; unfortunately, π is a transcendental number and we cannot construct it (or its square-root) using just a straight edge and compass. Thus the ancient Greek mathematicians would object to an assertion that this has a solution as it is non-constructible (given the tools they allow).

The two examples above are not random, unimportant problems. Both played a key role in the development of mathematics. The first led to the introduction of complex numbers and eventually the Fundamental Theorem of Arithmetic, which states that any polynomial of degree n with complex coefficients has exactly n complex roots (a complex number z can be written as $z = x + iy$, with x and y real). What this means is that once we introduce a new symbol to solve $x^2 + 1 = 0$, we can not only solve all quadratic equations, but also all cubic, quartic and any finite degree polynomial – not a bad return for the introduction of just one number! Our second example is one of the three famous constructions that the Greeks desired but could not find. This problem is equivalent to squaring the circle: can you construct (using straight edge and compass) a square whose area equals that of a circle of radius 1? (The other two problems are doubling a cube and trisecting an arbitrary angle, which are also both impossible.)

While our two above problems don't have 'standard' solutions, they are at least solvable. This is not always the case. Consider for example $e^x = 0$. Even if we allow x to be complex there are no solutions, so it is possible to write down equations without roots. Interestingly, $e^x = a$ can be solved for any complex a other than zero; perhaps the most famous choice of a is -1, which leads to the famous and beautiful formula $e^{\pi i} = -1$.

When given an equation, there are three natural questions to ask: Is there a solution? How many solutions are there? Can we find them? After our discussion above, we see that we must restrict the space of equations we study in order to make progress. A popular and important class of problems are Diophantine equations, which ask for solutions in rational numbers to the equation $p(x_1, \dots, x_n) = 0$, where p is a polynomial with rational coefficients. These equations have intrigued mathematicians from the dawn of the subject to the present day; two simple examples are the Pythagorean Theorem and Fermat's Last Theorem (if $n > 2$ is an integer then the only integer solutions to $x^n + y^n = z^n$ have $xyz = 0$).

In 1900 the Second International Congress on mathematics was held in Paris. David Hilbert, one of the greatest of his or any generation, gave an influential address where he listed some of the most important problems in mathematics. This list has motivated and shaped the course of mathematical research ever since. To this day, one of the highest honors someone can receive is joining the Hilbert Class, the elite list of people who have solved one of these 23 problems.

Hilbert's tenth problem dealt with our questions above: *Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.* Unfortunately, it turns out that even this is asking too much; in 1970 Matiyasevich completed a chain of ideas of many mathematicians (including Julia Robinson, Martin Davis, and Hilary Putnam), proving that Hilbert's tenth problem is unsolvable.

Centennial Problem 1970. *Proposed by Steven J. Miller.*

The main problem for this year is doing double duty, serving as the problem for 1994 as well! However, as the solution involves not just the Fibonacci numbers but also Zeckendorf's decomposition theorem, this provides a nice opportunity to talk about some of my favorite subjects. Zeckendorf's theorem states that if we write the Fibonaccis as 1, 2, 3, 5, 8, ... then every positive integer can be written uniquely as a sum of non-adjacent Fibonacci numbers. The standard proof is to use a greedy algorithm: given an m, remove the largest Fibonacci number (say F_n) at most m. If the difference is non-zero remove the largest Fibonacci possible; if that was F_{n-1} then we could have removed F_{n+1}, a contradiction.

Here is an outline for another approach. I call the following the cookie problem, though it's more commonly referred to as the stars and bars problems: *How many ways are there to divide C identical cookies among P people, where all that matters* *is how many cookies someone gets, not which cookies.* This is equivalent to solving $x_1 + \cdots + x_P = C$ with each x_i a non-negative integer. In [2] this is used to not only prove Zeckendorf's theorem, but also to show that if we look at all integers between the n^{th} and $(n+1)^{\text{st}}$ Fibonacci number that, as $n \to \infty$, the number of summands in the Zeckendorf decomposition becomes normally distributed! Can you figure out how to prove Zeckendorf's theorem from knowing that the number of solutions to this Diophantine equation is $\binom{C+P-1}{P-1}$? Can you find an elementary proof that the claimed number of solutions is correct?

REFERENCES

[1] Golden Museum, "Hilbert's Tenth Problem: a History of Mathematical Discovery (Diophantus, Fermat, Hilbert, Julia Robinson, Nikolay Vorob'ev, Yuri Matiyasevich)", http://www.goldenmuseum.com/1612Hilbert_engl.html.

[2] M. Koloğlu, G. S. Kopp, S. J. Miller and Y. Wang, *On the number of summands in Zeckendorf decompositions* Fibonacci Quarterly **49** (2011), no. 2, 116–130. http://arxiv.org/pdf/1008.3204.pdf.

[3] Y. Matiyasevich, "My collaboration with Julia Robinson", The Mathematical Intelligencer **14** (1992), no. 4, 38–45, (corrections in volume 15, no. 1, 1993, p.75). Available online: http://logic.pdmi.ras.ru/~yumat/Julia/.

[4] M. Vsemirnov, "Hilbert's Tenth Problem page!", last modified March 14, 2007. http://logic.pdmi.ras.ru/Hilbert10/.

1974

Rubik's cube

In 1974, Ernö Rubik invented the "Rubik's cube," a mechanical puzzle that quickly became popular around the world. It is easy to scramble a cube with just a few turns; figuring out how to restore the six faces takes much more work. The first World Championships took place in 1982; the winner Minh Thai, of the USA, won with a best time of 22.95 seconds. The Rubik's cube has seen a revival in the past decade, and the founding of the World Cube Association (WCA) in 2005 has greatly increased the prevalence of cube competitions. The current world record is a single solve of 5.55 seconds, held by Mats Valk of the Netherlands. Feliks Zemdegs, of Australia, holds the record for the best average of five solves, with a time of 7.53 seconds. Aside from the thrill that comes with speed and competitions, the Rubik's cube is an interesting mathematical object. The cube contains over 43 quintillion $(43 \cdot 10^{18})$ possible states, yet every state can be solved in 20 moves or fewer. This was shown after many years of work in 2010, requiring lots of computing power and mathematics. The Rubik's Cube is a concrete example of a mathematical object called a "group." The elements of the group are sequences of moves, and we can "multiply" two elements together by doing one sequence of move after the other. It is possible to solve an entire cube using only group theory; the notion of a commutator (moves of the form $X \cdot Y \cdot X^{-1} \cdot Y^{-1}$) is especially powerful.

Centennial Problem 1974. *Proposed by Alan Chang, Princeton University.*

(a) Suppose you start with a solved Rubik's cube. Prove that every (finite) sequence of turns on the cube, if repeated enough times, will get you back to the solved state. (b) Observe that each of the three dimensions of the Rubik's cube has two "cuts" (in order to produce three layers). We'll say that a Rubik's cube "has cuts at 1/3 and 2/3." If you wanted to turn a face of the cube, you must turn along one of these cuts. Similarly, a $4 \times 4 \times 4$ cube has cuts at 1/4, 2/4, and 3/4. Suppose instead that we have a cube which has a cut at α for *every* $\alpha \in [0, 1]$. (Clearly, there is no way to make this as a mechanical puzzle!) Now, is it true that any finite

sequence of moves, if repeated enough times, will get you back to a solved state?
Acknowledgements: This problem would not have been possible without the help of the following: (1) Steven J. Miller suggested looking at an infinite variation of (a). (2) A dinner discussion with a large group of SMALL REU students at Williams College, Summer '13, generated lots of ideas. (3) Scott Sicong Zhang helped simplify the proof of (b).

REFERENCES

[1] Rubik's cube homepage, http://www.rubiks.com/.

1978

Mandelbrot Set or Video Games

Centennial Problem 1978. *Proposed by Possibly Chris Long if video games.*

REFERENCES

[1] M. Aigner and G. M. Ziegler, "Proofs from The Book ", Springer-Verlag, Berlin, 1998.

1982

Two Envelope Problem

Martin Gardner popularizes the problem in his book *Aha! Gotcha*.

Connection with Bayes.

Two people, equally rich, meet to compare the contents of their wallets. Each is ignorant of the contents of the two wallets. The game is as follows: whoever has the least money receives the contents of the wallet of the other (in the case where the amounts are equal, nothing happens). One of the two men can reason: "I have the amount A in my wallet. That's the maximum that I could lose. If I win (probability 0.5), the amount that I'll have in my possession at the end of the game will be more than 2A. Therefore the game is favourable to me." The other man can reason in exactly the same way. In fact, by symmetry, the game is fair. Where is the mistake in the reasoning of each man? (Taken from Wikipedia, probably taken from Aha! Gotcha.)

Centennial Problem 1982. *Proposed by .*

REFERENCES

[1] M. Aigner and G. M. Ziegler, "Proofs from The Book ", Springer-Verlag, Berlin, 1998.

1986

Sudokus and Look and Say

Long ago movie theaters would have double features, where people could see two films for the price of one. Opened in 1936, the Astor Theatre in Melbourne, Australia is one of the few places where people can still catch a double feature. In honor of its 50th anniversary, we present a mathematical double feature: two 'recreational' math topics for the price of one!

It's hard today to find someone who hasn't heard of Sudokus. Their rise to popularity began in 1986 with the puzzle company Nikoli in Japan, and have become so ubiquitous that they now share space with crossword puzzles in newspapers and airline magazines. There is a lot of terrific mathematics about them. The first natural question to ask is how many distinct puzzles there are. For example, if we switch all 1s and 9s we get a puzzle that looks different, but isn't. There are other transformations we can do, such as rotating the puzzle by 90 degrees, or flipping about the middle row, or interchanging the first and third row, ... Up to symmetries, there are 5,472,730,538 essentially different puzzles. Another natural question is what is the minimal number of clues which must be given in order to uniquely determine how a Sudoku is filled. This was recently proved to be 17 by Gary McGuire, Bastian Tugemann and Gilles Civario. For more information, see [4, 5, 6, 8].

For our second feature, consider the famous 'See and Say' (or 'Look and Say') sequence of Conway. The first few terms are 1, 11, 21, 1211, 111221, 312211, 13112221, 1113213211. The pattern becomes clear if you say it aloud: after the first term, each term comes from saying the previous aloud. The first term is one. The second term is one one, which is how we would say the number of numbers in the first term (i.e., we have one number and that number is one). The next term is two ones, and we get that by saying the number of each number in the second term, followed by one two and one one. Conway and his colleagues proved a number of remarkable facts about this simple sequence. The following is from the abstract of a talk on the subject given by Alex Kontorovich at Columbia on March 23, 2004: *He found that the sequence decomposed into certain recurring strings. Categorizing these 92 strings and labeling them by the atoms of the periodic table (from Hydrogen to Uranium), Conway was able to prove that the asymptotic length of the sequence grows exponentially, where the growth factor (now known as Conway's Constant) is found by computing the largest eigenvalue of a* 92×92 *transition matrix. Even more remarkable is the Cosmological Theorem, which states that regardless of the starting string, every Look-And-Say sequence will eventually decay into a compound of these 92 atoms, in a bounded number of steps. Conway writes that, although two independent proofs of the Cosmological Theorem were verified, they were lost in writing! It wasn't until a decade later that Doron Zeilberger's paper (coauthored with his computer, Shalosh B. Ekhad) gave a tangible proof of the theorem. We will discuss this weird and wonderful chemistry, and some philosophical consequences. The only prerequisite is basic linear algebra.* We urge the reader to visit the links and read the references [1, 2, 3, 7] and learn more about these!

Centennial Problem 1986. *Proposed by Steven J. Miller, Williams College.*

From the abstract of [5]: *The sudoku minimum number of clues problem is the following question: what is the smallest number of clues that a sudoku puzzle can have? For several years it had been conjectured that the answer is 17. We have performed an exhaustive computer search for 16-clue sudoku puzzles, and did not ?nd any, thus proving that the answer is indeed 17. In this article we describe our method and the actual search. As a part of this project we developed a novel way for enumerating hitting sets. The hitting set problem is computationally hard; it is one of Karps 21 classic NP-complete problems. A standard backtracking algorithm for finding hitting sets would not be fast enough to search for a 16-clue sudoku puzzle exhaustively, even at todays supercomputer speeds. To make an exhaustive search possible, we designed an algorithm that allowed us to efficiently enumerate hitting sets of a suitable size.* One can consider larger and larger Sudokus. The next largest is the 16×16, though in general we can look at $n^2 \times n^2$ grids. How does the minimum number of clues grow with n? Can you find any lower bounds? Any upper bounds?

Let's consider variants of the Look and Say sequence. For example, what if instead of saying two three for 33 we say three two, so we are saying things backwards? Note that there's no difference for 1, 22, or 333 but there is a difference for 33. If we again start with 1 the first few terms are now 1, 11, 12, 1121, 122111, 112213, 12221131; interestingly each term is the reverse of the corresponding term in the original sequence (1, 11, 21, 1211, 111221, 312211, 13112221). Does this pattern hold forever? What if instead whenever we have just one of a number we just write that number? In this case if we start with 1 we always have 1, but if we have 11 it would go to 21, and then all subsequent terms are also 21. If we start with 112 then the next term is 212, followed by 212, which then stabilizes. Prove or disprove: if we start with a finite string composed of 1s, 2s and 3s, does the sequence eventually stabilize (so that all terms from some point onward are the same)?

REFERENCES

[1] J. H. Conway, "The Weird and Wonderful Chemistry of Audioactive Decay", Eureka **46** (1986), 5–18.

[2] S. B. Ekhad and D. Zeilberger, "Proof of Conway's lost cosmological theorem", Electronic Research Announcements of the AMS **3** (1997), 78–82.

[3] Ó. Martín, "Look-and-Say Biochemistry: Exponential RNA and Multistranded DNA", American Mathematical Monthly **113** (2006), no. 4, 289–307. http://web.archive.org/web/20061224154744/http://www.uam.es/personal_pdi/ciencias/omartin/Biochem.PDF.

[4] Math Explorer's Club, "The Math Behind Sudoku: References", http://www.math.cornell.edu/~mec/Summer2009/Mahmood/References.html.

[5] G. McGuire, B. Tugemann and G. Civario, "There is no 16-Clue Sudoku: Solving the Sudoku Minimum Number of Clues Problem", preprint 2013. http://arxiv.org/abs/1201.0749.

[6] E. Russell and F. Jarvis, "There are 5472730538 essentially different Sudoku grids... and the Sudoku symmetry group", Mathematical Spectrum **39** (2006), 54–58. http://www.afjarvis.staff.shef.ac.uk/sudoku/sudgroup.html.

[7] Wikipedia, "Look and Say", http://en.wikipedia.org/wiki/Look-and-say_sequence.

[8] Wikipedia, "Sudoku", http://en.wikipedia.org/wiki/Sudoku.

1990

The Sleeping Beauty Problem

One of the most enjoyable parts of writing problems is seeing the conversations they generate. In recent times one of the most famous is the Monty Hall Problem, which is given in 1990. There was vigorous debate in the mathematics community and beyond as to what was the right answer. The following fun problem continues this tradition and is also from 1990, though not as widely known. A variant first appeared in Zuboff's article in Inquiry: An Interdisciplinary Journal of Philosophy; on a personal note, as a father with a young daughter who loves the Disney princesses, it's a nice way to use them to highlight math.

Centennial Problem 1990. *Proposed by Adam Elga, Princeton University.*

The Sleeping Beauty Problem. The Sleeping Beauty problem: Some researchers are going to put you to sleep. During the two days that your sleep will last, they will briefly wake you up either once or twice, depending on the toss of a fair coin (Heads: once; Tails: twice). After each waking, they will put you to back to sleep with a drug that makes you forget that waking. When you are first awakened, to what degree ought you believe that the outcome of the coin toss is Heads?

REFERENCES

[1] A. Elga, "Self-locating Belief and the Sleeping Beauty problem", Analysis **60** (2000), no. 2, 143–147. http://www.princeton.edu/~adame/papers/sleeping/sleeping.pdf.

[2] A. Zuboff, "One self: The logic of experience", Inquiry: An Interdisciplinary Journal of Philosophy 33 (1990), no. 1, 39–68.

1994

AIM

In 1994 John Fry funded the creation of AIM, the American Institute of Mathematics. Since 2002 it has been one of now eight institutions that are part of the National Science Foundation's Mathematical Sciences Institute Program (the others are the Institute for Advanced Study (IAS) in Princeton, the Institute for Computational and Experimental Research in Mathematics (ICERM) in Providence, the Institute for Mathematics and its Applications (IMA) in Minneapolis, the Institute for Pure and Applied Mathematics (IPAM) in LA, the Mathematical Biosciences Institute (MBI) in Columbus, Mathematical Sciences Research Institute (MSRI) at Berkeley, and the Statistical and Applied Mathematical Sciences Institute (SAMSI) at Research Triangle Park in North Carolina). Since their founding they have brought together many scientists and fostered long-term collaborations, which have resulted in solutions to many important problems. They have also run many programs on mathematical outreach, broadening participation and helping excite the next generation. The following text is from AIM's homepage; for more information, including some stories on recent spectacular successes, see [1, 2, 3].

> *The mission of AIM is to advance mathematical knowledge through collaboration, to broaden participation in the mathematical endeavor, and to increase the awareness of the contributions of the mathematical sciences to society.*
>
> *Since 2002 AIM has been part of the National Science Foundation (NSF) Mathematical Sciences Institutes program. AIM receives funding from NSF to hold weeklong focused workshops in all areas of the mathematical sciences. In 2007 a program called SQuaREs which brings small research groups to AIM was developed. Each year twenty workshops are hosted at the institute and over thirty small research groups.*
>
> *AIM strives to broaden participation in the mathematical sciences at every level, from supporting the research of professional mathematicians working on the most important mathematical problems of our day to encouraging young students to get excited about math and become the STEM professionals of the future.*
>
> *AIM created the Math Teachers' Circle Network to encourage problem solving in middle schools, and now there are nearly 60 active Math Teachers' Circles nationwide. Recently, AIM announced a new partnership with the Julia Robinson Mathematics Festivals. At the local level, AIM provides support and leadership to numerous students, teachers, and organizations throughout the South Bay and Silicon Valley communities.*

Centennial Problem 1998. *Proposed by Steven J. Miller, Williams College.*

There are so many good stories arising from work at AIM that it's hard to choose; I chose the following as it connects with an earlier problem from this set of 100th anniversary problems (Hilbert's tenth problem, see 1970), as well as one from the previous set (the founding of Sage, see 2005). For more details, see the article "A Trillion Triangles" [4].

The problem is deceptively simple to state: *What positive integers are the areas of a right triangle with rational sides?* In other words, we want to solve the system of equations $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$, where a, b and c are rational numbers and

n is an integer. If you prefer just one equation we can oblige by using the famous trick of subtracting and squaring: $(a^2+b^2-c^2)^2+(\frac{1}{2}ab-n)^2=0$. Such n are called congruent numbers, and this is often called the *congruent number problem*.

Given a right triangle we can always find the corresponding congruent number (if the resulting number is rational and not an integer, we just rescale the sides). For example, the famous 3-4-5 triangle gives the congruent number 6, while 5-12-13 gives us 30. Are there infinitely many congruent numbers? If so which numbers are congruent numbers? As it turns out to be quite challenging to find such numbers, we can lower our goals and try to predict roughly how many there are. For example, find a function of x that is an excellent approximation to the number of congruent numbers at most x as $x \to \infty$. Read the article [4] and the links on the right (which describe the computers and the theory of congruent numbers). Can you do better? The research groups there were able to resolve the first *trillion* cases. One of the greatest difficulties in this was the enormous size of the computations. From the article: *The advance was made possible by a clever technique for multiplying large numbers. The numbers involved are so enormous that if their digits were written out by hand they would stretch to the moon and back. The biggest challenge was that these numbers could not even fit into the main memory of the available computers, so the researchers had to make extensive use of the computers' hard drives.* One of the teams used the computer Sage at the University of Washington (see the problem from 2005).

Can you replicate their work? How many cases can you resolve? Can you extend and get the up to a quadrillion? The last question is particularly important as it would allow us to further check the conjectured growth formula for the number of congruent numbers, which does a great job in the range investigated to date.

REFERENCES

[1] AIM, Homepage, http://www.aimath.org.
[2] AIM, News, http://aimath.org/aimnews/.
[3] AIM, Newsletter, http://aimath.org/aimnews/newsletter/.
[4] AIM, "A Trillion Triangles", http://aimath.org/news/congruentnumbers/.

1998

The Kepler Conjecture

The Kepler problem concerns the densest packing of equal spheres in space. In one or two dimensions the problem is easy; for two dimensions the best packing is to tile the plane with hexagons, and inscribe the circles at the centers. In three dimensions, however, the problem becomes enormously more difficult. After a little experimentation one quickly comes to believe that the best solution is to start with a hexagonal packing, with the center of the spheres at the centers of the hexagons. This gives us our first layer. The next layer is another such packing, but shifted so the the new spheres go into the valleys of the first layer. Continuing this process, one gets a packing whose density is $\frac{\pi}{3\sqrt{2}} \approx 74.04\%$. Kepler conjectured in 1611 in "On the six-cornered snowflake" (available online at http://www.thelatinlibrary.com/kepler/strena.html) that this packing is optimal. The problem was brought to his attention by Thomas Harriot, who had been asked by Sir Walter Raleigh what was the optimal way to stack cannonballs on the ship. Not surprisingly this is known as the cannonball packing (and close approximations can be seen in various fruit displays at stores). The problem was posed earlier than Fermat's Last Theorem and fell shortly afterwards, making it an open, active problem for a longer period of time. A landmark solution to the problem was put forth in a series of six preprints by

Thomas C. Hales and Samuel P. Ferguson in the Mathematics arXiv in 1998, where they proved this (plus uncountably many other packings of equal density) give the best density. After a long peer review process, revised versions of the six papers were published in 2006 in Discrete and Computational Geometry. Problems of packing small spheres in containers are already very difficult.

Centennial Problem 1998. *Proposed by Jeffrey Lagarias, University of Michigan.*

Determine the minimal side of a cube $R(n)$ sufficient to pack completely inside n unit radius spheres, for $1 \le n \le 20$. If you cannot get exact answers, determine upper and lower bounds.

REFERENCES

[1] Th. Gensane, "Dense packings of equal spheres in a cube", Elect. J. Combin. **11** (2004), no. 1, Research paper 33.
http://www.combinatorics.org/ojs/index.php/eljc/article/view/v11i1r33/pdf.

[2] A. Joós, "On the packing of 14 congruent spheres in a cube", Geom. Dedicata **140** (2009), 49–80.

2002

PRIMES in P

Given an integer larger than 1, how quickly can you tell whether it is prime or composite? Everyone knows a method, namely divide the number by $2, 3, \dots$. If you discover a factor, the number is composite, and if you reach the square root of the candidate without finding a factor, it's prime. Some numbers, like the set of even numbers, get recognized instantly. But the method takes about $\sqrt{n}$ steps to recognize that n is prime, when it is so. This is impractical for $n > 10^{30}$, say.

The question is if there is a "polynomial-time" procedure to distinguish between primes and composites, where it is not necessary to find a factor of a composite, only merely to recognize that it is composite. A number n is presented to us by its digits (usually decimal or binary) and the length of this representation for n is proportional to $\log n$. So polynomial time means that there should be constants A, B so that the the total number of elementary steps performed by the algorithm on n is at most $A(\log n)^B$.

Using Fermat's little theorem to the base 2 (that is, when p is an odd prime, $2^{p-1} \equiv 1 \bmod p$) suggests itself, since verifying the congruence can be accomplished in polynomial time (see the entry from 2010 on Carmichael numbers). However, some composites also satisfy this congruence. By using certain elaborations of Fermat's little theorem (like using that the only square roots of 1 mod p for an odd prime p are ± 1 and that this is untrue mod$n$ if n is divisible by two different odd primes), one can construct a random procedure that expects to recognize composites (and prove that they are composite) in polynomial time. (Examples are the Solovay–Strassen test or the Miller–Rabin test.) If such a random algorithm is tried out on a prime input, it grinds away looking for a proof that it is composite, and never finds such a proof. You can conclude that either the number is prime, or it is composite and you have been very unlucky in finding a proof.

On the other hand, we also have the Adleman–Huang test, a random procedure that expects to find a proof of primality for a prime input in polynomial time. This is much more difficult, using very deep mathematics.

We would like to "de-randomize" the problem. That is, we would like a *deterministic* polynomial-time algorithm that can distinguish between primes and composites. Over the years there were some close calls, but it wasn't until an electrifying announcement from India in 2002 that we had an answer. Manindra Agrawal and his two undergraduate honors students, Neeraj Kayal and Nitin Saxena, gave a fairly simple deterministic polynomial-time algorithm that distinguishes primes from composites. It involves a generalization of Fermat's little theorem to the ring of polynomials over a prime finite field modulo an irreducible polynomial. The algorithm is accessible and the reader is encouraged to check it out in the original paper or in one of the secondary references.

Centennial Problem 2002. *Proposed by Carl Pomerance, Dartmouth College.*

Agrawal, Kayal, and Saxena were successful in de-randomizing the prime recognition problem. Here is another simple problem where there is a polynomial-time random algorithm, but we don't know yet if there is a polynomial-time deterministic algorithm. Given an odd prime p, find an integer a such that a is a quadratic non-residue for p; that is, the congruence $x^2 \equiv a \bmod p$ has no integer solution x. We seek a quadratic non-residue, and they are not at all scarce! In fact, half of the non-zero residues mod$p$ fit the bill. In addition, a candidate can be quickly checked (in polynomial time) via either Euler's criterion or the law of reciprocity for Jacobi symbols. Thus, the algorithm of randomly selecting nonzero residues a until you are successful expects to succeed in 2 tries! A possible deterministic algorithm sequentially tries small numbers for a until a good one is found. This works well for a large proportion of the primes. For example, one of $-1, 2, 3, 5$ is a quadratic non-residue for an odd prime p unless $p \equiv 1$ or 49 mod 120. Conjecturally the procedure of trying small values of a till success works in polynomial time, but this is only known under the Extended Riemann Hypothesis. Another possible strategy: Start with -1 and sequentially take modular square roots until a non-square is found. Fine, but we know no method to take modular square roots in deterministic polynomial time, unless one pre-supposes an oracle that give you a quadratic non-residue! Is there some other de-randomization of this problem that can be proved to run in polynomial time? No one knows.

REFERENCES

[1] M. Agrawal, N. Kayal and N. Saxena, "PRIMES is in P", Annals of Mathematics (2) **160** (2004), 781–793.
http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf.

[2] R. Crandall and C. Pomerance, Prime numbers: a computational perspective, 2nd ed., Springer, New York, 2005.

[3] A. Granville, "It is easy to determine if a given number is prime", Bull. Amer. Math. Soc. 42 (2004), 3–38. http://www.dms.umontreal.ca/~andrew/PDF/Bulletin04.pdf.

[4] C. Pomerance, "Primality testing: variations on a theme of Lucas", Congressus Numerantium 201 (2010), 301–312. http://cm.bell-labs.com/cm/ms/who/carlp/PS/primalitytalk5.ps.

2006

Centennial Problem 2006. *Proposed by .*

REFERENCES

[1] M. Aigner and G. M. Ziegler, "Proofs from The Book ", Springer-Verlag, Berlin, 1998.

2010

Carmichael Numbers

E-commerce as we know it would be impossible without the ability to securely transmit information. As many of these schemes involve prime numbers, primality tests (methods to determine if a number is prime) are extremely important and have been the center of much research over the years. One popular method involves Fermat's little Theorem, which asserts that for each prime p and every integer a relatively prime to p, we have $a^{p-1} \equiv 1 \bmod p$. It is very easy to check this congruence despite the presence of a potentially huge power. The idea is if one has $a^u \bmod p$ and $a^v \bmod p$, then in one simple step one can obtain $a^{u+v} \bmod p$, using arithmetic with integers at most p^2. So, one builds up to the high exponent $p-1$ by an "addition ladder", where each term after the first (which is 1), is the sum of two prior terms. If one actually does this calculation for some a and p (say $a = 2$ and $p = 91$), one may find that $a^{p-1} \not\equiv 1 \bmod p$, and then conclude that p is not prime afterall, despite the misleading notation of using the letter p. Thus we have the strange situation where a simple calculation can determine that a number, in this case 91, is composite *without finding any factors!*

Is this simple test iron clad? No, it is not as $2^{340} \equiv 1 \bmod 341$, but 341 is composite. In fact, there are particularly troublesome numbers, the first is 561, which are composite, yet $a^{560} \equiv 1 \bmod 561$ for every integer a relatively prime to 561. These are called *Carmichael numbers*, and it was proved in 1994 by Alford, Granville, and Pomerance that there are infinitely many of them. A starting point for the proof is the following if-and-only-if criterion for n to be a Carmichael number: it is composite, square-free, and for each prime p dividing n we have $p-1$ divides $n-1$. Thus we need more powerful methods than Fermat's little Theorem (see for example the problem from 2002).

Centennial Problem 2010. *Proposed by Carl Pomerance, Dartmouth College.*

(1) Let $b(n)$ be the number of integers a in $[1, n]$ with $a^n \equiv a \bmod n$. Show that $b(n) = n$ if and only if n is 1, a prime, or a Carmichael number. Somewhat harder: show that if n is a non-Carmichael composite, then $b(n) \leq \frac{2}{3}n$. (2) Say n is a "taxi cab Carmichael number" if n is composite and $a^{(n-1)/2} \equiv \pm 1 \bmod n$ for every integer a relatively prime to n. (The first example is $n = 1729$, the famous number of Hardy's taxi cab when he was visiting Ramanujan in the hospital. Look up the story in the reference below!) Show that if n is a taxi cab Carmichael number, then $a^{(n-1)/2} \equiv 1 \bmod n$ for all integers a relatively prime to n; that is, the "-1" in the definition never occurs.

REFERENCES

[1] W. R. Alford, A. Granville and C. Pomerance, "There are Infinitely Many Carmichael Numbers", Annals of Mathematics **139** (1994), 703–722. http://www.math.dartmouth.edu/~carlp/PDF/paper95.pdf.

[2] G. H. Hardy, "A mathematician's apology", First Electronic Edition, Version 1.0 March 2005, published by the University of Alberta Mathematical Sciences Society. http://www.math.ualberta.ca/mss/misc/A%20Mathematician's%20Apology.pdf.