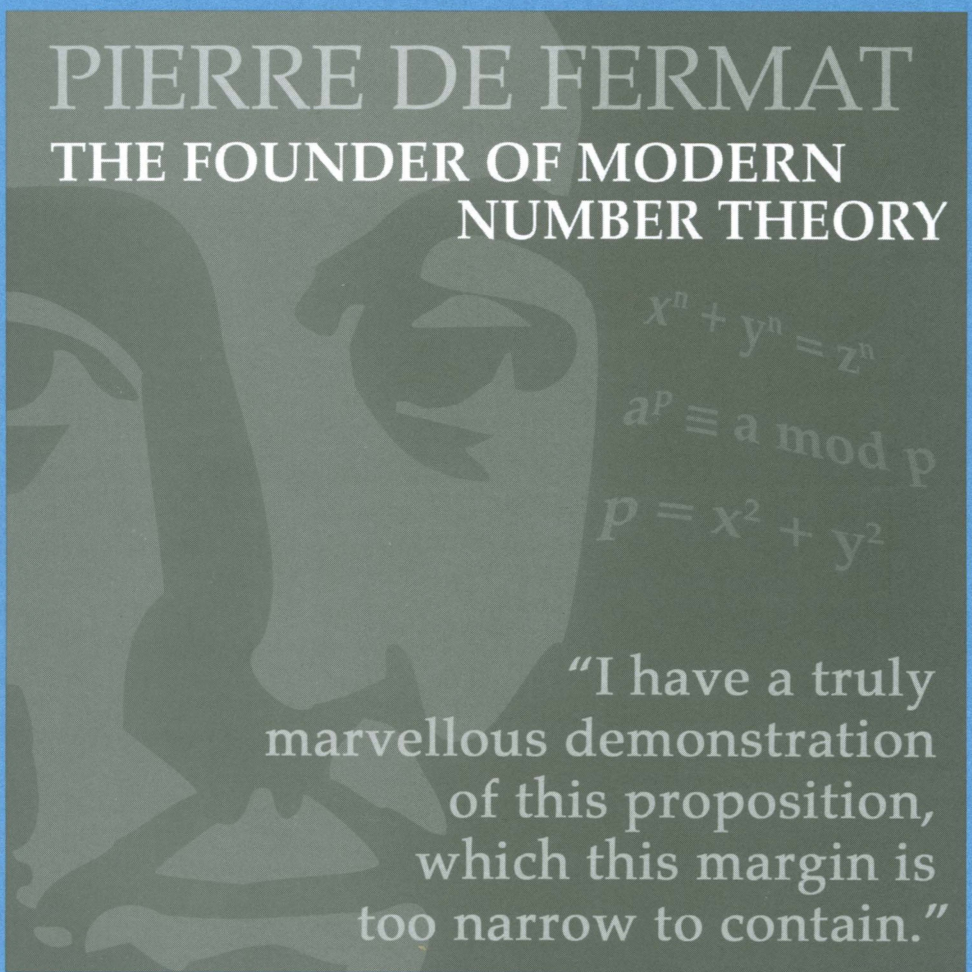
Vol. 78, No. 1, February 2005

MATHEMATICS MAGAZINE



- Fermat: The Founder of Modern Number Theory
- The Singled Out Game
- Height and Excess of Pythagorean Triples

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

EDITORIAL POLICY

Mathematics Magazine aims to provide lively and appealing mathematical exposition. The *Magazine* is not a research journal, so the terse style appropriate for such a journal (lemma-theorem-proof-corollary) is not appropriate for the *Magazine*. Articles should include examples, applications, historical background, and illustrations, where appropriate. They should be attractive and accessible to undergraduates and would, ideally, be helpful in supplementing undergraduate courses or in stimulating student investigations. Manuscripts on history are especially welcome, as are those showing relationships among various branches of mathematics and between mathematics and other disciplines.

A more detailed statement of author guidelines appears in this *Magazine*, Vol. 74, pp. 75–76, and is available from the Editor or at www.maa.org/pubs/mathmag.html. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, or published by another journal or publisher.

Submit new manuscripts to Allen Schwenk, Editor-Elect, Mathematics Magazine, Department of Mathematics, Western Michigan University, Kalamazoo, MI, 49008. Manuscripts should be laser printed, with wide line spacing, and prepared in a style consistent with the format of *Mathematics Magazine*. Authors should mail three copies and keep one copy. In addition, authors should supply the full five-symbol 2000 Mathematics Subject Classification number, as described in *Mathematical Reviews*.

Cover image: *Fermat ponders great equations*, by Neil Mitchell, who studies graphic arts at West Valley College. Mathematics is not Neil's strong point but he thoroughly enjoys the Donald Duck film "Donald in Mathmagic Land." Neil's work was directed by Jason Challas, who teaches beginning drawing and design at WVC.

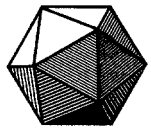
AUTHORS

Israel Kleiner is Professor Emeritus of mathematics at York University in Toronto. He received his Ph.D. in ring theory from McGill University. His research interests for the past twenty years have been the history of mathematics, mathematics education, and their interface. He was for many years coordinator of an in-service Master's Programme for teachers. Recently he served as Vice President and Council member of the Canadian Society for the History and Philosophy of Mathematics. He was awarded the MAA's Pólya, Allendoerfer, and Ford prizes.

Kennan Shelton received his B.S. from the University of Central Arkansas and his Ph.D. from the University of North Carolina, Chapel Hill. His areas of interest include ergodic theory, combinatorial game theory, theory of computation and finding ways to win over women with mathematics.

Darryl McCullough is a professor of mathematics at the University of Oklahoma. His usual research topics are in low-dimensional topology, but he became interested in Pythagorean triples while directing an undergraduate research project by Elizabeth Wade. A member of the MAA for many years, he served on its Board of Governors from 1996 to 1999. He and his wife Laurie are happily vegan.

Vol. 78, No. 1, February 2005



MATHEMATICS MAGAZINE

MATHEMATICS MAGAZINE (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, D.C. 20036 and Montpelier, VT, bimonthly except July/August.
The annual subscription price for *MATHEMATICS MAGAZINE* to an individual member of the Association is $131. Student and unemployed members receive a 66% dues discount; emeritus members receive a 50% discount; and new members receive a 20% dues discount for the first two years of membership.)

Subscription correspondence and notice of change of address should be sent to the Membership/ Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036. Microfilmed issues may be obtained from University Microfilms International, Serials Bid Coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

Advertising correspondence should be addressed to Frank Peterson (*FPetersonj@aol.com*), Advertising Manager, the Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036.

Periodicals postage paid at Washington, D.C. and additional mailing offices.

Postmaster: Send address changes to Membership/ Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036-1385.

Printed in the United States of America

ARTICLES

Fermat: The Founder of Modern Number Theory

ISRAEL KLEINER
Department of Mathematics and Statistics
York University
Toronto, ON M3J 1P3
kleiner@rogers.com

Fermat, though a lawyer by profession and only an "amateur" mathematician, is regarded as the founder of modern number theory. What were some of his major results in that field? What inspired his labors? Why did he not publish his proofs? How did scholars attempt to reconstruct them? Did Fermat have a proof of Fermat's Last Theorem? What were the attitudes of 17th-century mathematicians to his number theory? These are among the questions we will address.

We know that work on Fermat's Last Theorem led to important developments in mathematics. What of his other results? How should we view them in the light of the work of subsequent centuries? These issues will form another major focus of the paper.

Number theory was Fermat's mathematical passion. His interest in the subject was aroused in the 1630s by Bachet's Latin translation of Diophantus' famous treatise *Arithmetica* (ca. 250 C.E.). Bachet, a member of an informal group of scientists in Paris, produced an excellent translation, with extensive commentaries.

Unlike other fields to which he contributed, Fermat (1607–65) had no formal publications in number theory. (Fermat's date of birth is usually given as 1601; recently it has been suggested that the correct date is 1607 [**5**].) His results, and very scant indications of his methods, became known through his comments in the margins of Bachet's translation and through his extensive correspondence with leading scientists of the day, mainly Carcavi, Frenicle, and Mersenne. Fermat's son Samuel published his father's marginal comments in 1670, as *Observations on Diophantus*. A fair collection of Fermat's correspondence has also survived. Both are available in his collected works [**33**]. But they reveal little of his methods and proofs. As his biographer Mahoney notes ruefully [**25**, pp. 284–285]:

> Fermat's secretiveness about his number theory makes the historian's task particularly difficult. In no other aspect of Fermat's career are the results so striking and the hints at the underlying methods so meager and disappointing. It is the results—the theorems and conjectures—and not the methods that drew the attention of men such as Euler, Gauss, and Kummer.

Weil, who wrote a masterful book analyzing (among other authors) Fermat's number-theoretic work, speculates about its lack of proofs [**35**, p. 44]:

> It is clear that he always experienced unusual difficulties in writing up his proofs for publication; this awkwardness verged on paralysis when number theory was concerned, since there were no models there, ancient or modern, for him to follow.

It must be emphasized, however, that Fermat did lay considerable stress on general methods and on proofs, as his correspondence makes clear. Weil gave plausible reconstructions of the proofs of some of Fermat's results. He did this by considering the often cryptic comments about his methods in letters to his correspondents, and, more importantly, by examining the proofs of Fermat's results in the works of Euler and Lagrange, in order to determine whether the methods used in these proofs were available to Fermat. As Weil put it in the case of one such reconstruction: "If we consult Euler... we see that Fermat could have proceeded as follows" [**35**, p. 64]. He cautions that "any attempt at reconstruction can be no more than a hit or miss proposition" [**35**, p. 115]. (For a *modern* interpretation of some of Fermat's number-theoretic work consult Weil [**35**, Chapter II, Appendices I–V].)

Fermat tried to interest his mathematical colleagues (notably Huygens, Pascal, Roberval, and Wallis) in number theory by proposing challenging problems, for which he had the solutions. (This was not an uncommon practice at the time.) He stressed that

> Questions of this kind [i.e., number-theoretic] are not inferior to the more celebrated questions in geometry [mathematics] in respect of beauty, difficulty, or method of proof [**20**, p. 286].

To no avail. Mathematicians showed little serious interest in number theory until Euler came on the scene some 100 years later. They were preoccupied with other subjects, mainly calculus. Their typical attitude during the 17th century was well expressed by Huygens [**35**, p. 119]: "There is no lack of better things for us to do." The mathematical community apparently failed to see the depth and subtlety of Fermat's propositions on numbers. And he provided little help in that respect.

Fermat's intellectual debts

What number-theoretic knowledge was available to Fermat when he started his investigations? His primary sources were surely Euclid's *Elements* and Diophantus' *Arithmetica* [**20, 21**]. There is no evidence (as far as we can ascertain) that Fermat knew of the considerable Indian, Chinese, or Moslem contributions to number theory—on, for example, linear Diophantine equations, the Chinese remainder theorem, and Pell's equation [**32**].

In books VII–IX of the *Elements* Euclid introduced some of the main concepts of the subject, such as divisibility, prime and composite integers, greatest common divisor, and least common multiple. He also established some of its major results, among them the Euclidean algorithm, the infinitude of primes, results on perfect numbers, and what some historians consider to be a version of the Fundamental Theorem of Arithmetic [**2**].

Diophantus' *Arithmetica* differs radically in style and content from Euclid's *Elements*. It contains no axioms or formal propositions and proofs. It has, instead, about 200 problems, each giving rise to one or more indeterminate equations—now called Diophantine equations, many of degree two or three. These are (in modern terms) equations in two or more variables, with integer coefficients, for which the solutions sought are integers or rational numbers. Diophantus sought rational solutions; nowadays, we are usually interested in integer solutions.

In fact, we have become interested in integer solutions mainly because of Fermat, who, contrasting his work with that of Diophantus, noted that "arithmetic has, so to speak, a special domain of its own, the theory of integral numbers" [**13**, p. 25]. (Of

course, Euclid, as well as Indian and Chinese mathematicians, dealt with *integers* in studying number-theoretic problems.) It should be stressed, however, that the study of *rational* solutions of Diophantine equations has become important in the last 100 years or so, with the penetration into number theory of the methods of algebraic geometry. Another of Fermat's legacies is his quest for *all* solutions of a given Diophantine equation; Diophantus was usually satisfied with a single solution.

We now come to discuss some of Fermat's major results, commenting on their sources and on developments arising from them.

Fermat's little theorem and factorization

Fermat's little theorem (Flt) states that $a^p - a$ is divisible by p for any integer a and prime p, or, equivalently, that $a^{p-1} - 1$ is divisible by p provided that a is not divisible by p. In post-1800 terms (after Gauss introduced the congruence notation), we can write the above as $a^{p-1} \equiv 1 \pmod{p}$, provided that $a \not\equiv 0 \pmod{p}$. Fermat stated several versions of this result, one of which he sent to Frenicle in 1640 [**35**, p. 56]:

> Given any prime p, and any geometric progression $1, a, a^2$, etc., p must divide some number $a^n - 1$ for which n divides $p - 1$; if then N is any multiple of the smallest n for which this is so, p also divides $a^N - 1$.

Fermat is thought to have arrived at Flt by studying perfect numbers [**13**, p. 19; **35**, pp. 54, 189]. Euclid showed that if $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is perfect (Proposition IX.36). This result presumably prompted Fermat to ask about the divisors of $2^n - 1$, which led him to the special case $a = 2$ of Flt, that is, that $2^{p-1} - 1$ is divisible by p, and thence to the general case.

Fletcher [**14, 15**] examines the correspondence between Frenicle and Fermat in 1640, and concludes that it was Frenicle's challenge to Fermat (delivered via Mersenne, who often acted as intermediary) concerning a specific perfect number, that was responsible for Flt. Frenicle asked: "And if he (Fermat) finds that it is not much effort for him to send you a perfect number having 20 digits, or the next following it" [**15**, p. 150]. Fermat responded that there is no such number, basing his answer on Flt. He wrote to Mersenne that "he would send [the proof] to Frenicle if he did not fear [it] being too long" [**35**, p. 56]. In his book Weil speculates how Fermat's proof might have gone, sketching two versions [**35**, pp. 56–57].

The dual problems of primality testing and factorization of large numbers are vital nowadays. The oldest method of testing if an integer n is prime, or finding a factor if n is composite, is by trial: test if there are divisors of n up to $\sqrt{n}$. The Sieve of Eratosthenes, devised ca. 230 B.C.E. for finding all primes up to a given integer, is based on this idea.

Fermat, too, was concerned with such problems. Note, for example, his interest in determining the primality of the Mersenne numbers, $2^n - 1$, and of what we now call Fermat numbers, $2^n + 1$. In 1643, in a letter probably addressed to Mersenne, he proposed the following problem: "Let a number, for example, 2,027,651,281, be given me and let it be asked whether it is prime or composite, and, in the latter case, of what numbers it is composed" [**25**, p. 326]. In the same letter he answered his own query by outlining what came to be known as *Fermat's factorization method*. It was inspired by his interest in the problem of representing integers as differences of two squares.

The factorization method is based on the observation that an odd number n can be factored if and only if it is a difference of two squares: If $n = ab$, with $a \geq b \geq 1$,

let $x = (a + b)/2$, $y = (a - b)/2$, then $n = x^2 - y^2$. Since n is odd, so are a and b, hence x and y are integers. The converse is obvious.

The algorithm works as follows: Given an integer n to be factored (we can assume without loss of generality that it is odd), we begin the search for possible x and y satisfying $n = x^2 - y^2$, or $x^2 - n = y^2$, by finding the smallest x such that $x \geq \sqrt{n}$. We then consider successively $x^2 - n$, $(x + 1)^2 - n$, $(x + 2)^2 - n$, ... until we find an $m \geq \sqrt{n}$ such that $m^2 - n$ is a square. The process must terminate in such a value, at worst with $m = [(n + 1)/2]^2$, yielding the trivial factorization $n \times 1$ (which comes from $[(n + 1)/2]^2 - n = [(n - 1)/2]^2$), in which case n is prime.

Fermat's factorization algorithm is efficient when the integer to be factored is a product of two integers that are close to one another. Moreover, it "contain[s] the key idea behind two of today's most powerful algorithms for factoring numbers with large prime factors, the Quadratic Sieve and the Continued Fraction Algorithms" [**10**, p. 58].

A look ahead As we mentioned, Fermat did not publish any proofs of his number-theoretic results, save one (see below). Most, including Flt, were proved by Euler in the next century. In 1801, Gauss gave an essentially group-theoretic proof of Flt, without using group-theoretic terminology. For a proof of the theorem using dynamical systems, see the recent note by Iga [**22**].

Fermat's little theorem turned out to be one of his most important results. It is used throughout number theory (an entire chapter of Hardy and Wright [**19**] discusses consequences of the theorem), so it is anything but a "little theorem," although the term has historical roots. For example, it can be used to prove that if -1 is a quadratic residue mod p, p an odd prime (that is, if $x^2 \equiv -1 \pmod{p}$ is solvable), then $p \equiv 1 \pmod{4}$; and it can be used to show that a given number p is composite without finding its factors, by finding a "small" a not divisible by p that does not satisfy Flt, though this is, in general, computationally not very efficient [**29**].

The converse of Flt is false, so the theorem cannot be used as a test of primality. But refinements and extensions of the theorem are at the basis of several primality tests. Here is one: The positive integer n is prime if and only if there is an a such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all primes q dividing $n - 1$ [**3**, p. 267]. A generalization of Flt to integers of cyclotomic fields was used by Adleman, Pomerance, and Rumely to yield a "deterministic algorithm" [**9**, p. 547] for testing for primality (1983), and the extension of the theorem to polynomials was the starting point for the recent (2002) spectacular achievement of Agrawal, Kayal, and Saxena in devising a test of primality in *polynomial time*. The test is rather slow, and of little practical value, but the result is of great theoretical interest [**9**]. The books by Bach and Shalit [**3**], Bressoud [**10**], and Riesel [**29**] deal with issues of primality and factorization.

Sums of squares

In Problem III.19 of the *Arithmetica*, which asks "to find four numbers such that the square of their sum *plus* or *minus* any one singly gives a square," Diophantus remarked that since 5 and 13 are sums of two squares, and $65 = 5 \times 13$, 65 is also a sum of two squares [**20**, p. 167]. He most likely had the identity $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$ in mind. (This was proved by Viète in the late 16th century using his newly created algebraic notation.) In Problem VI.14, "To find a right-angled triangle such that its area *minus* the hypotenuse or *minus* one of the perpendiculars gives a square," Diophantus noted in passing that "*This equation we cannot solve because 15 is not the sum of two [rational] squares*" [**20**, p. 237]. His remarks in

these problems appear to have prompted Bachet to ask which integers are sums of two squares, namely, for which integers n is the Diophantine equation $n = x^2 + y^2$ solvable.

Fermat took up the challenge. He reduced the question to asking which *primes* are sums of two squares, and claimed to have shown (recall that he gave no proofs) that every prime of the form $4k + 1$ is a sum of two squares, in fact, a unique such sum. He also stated results on the number of representations (if any) of an arbitrary integer as a sum of two squares [**35**, p. 70].

In a letter to Huygens in 1659, Fermat gave a slight indication of how he had proved the proposition about representing primes as sums of two squares, a result he had announced about twenty years earlier: He used, he said, his "method of infinite descent" (discussed in the next section), showing that if the proposition were not true for some prime, it would also not be true for a smaller prime, "and so on until you reach 5" [**35**, p. 67]. Weil observes (charitably to Fermat, we think) that "this may not have seemed quite enlightening to Huygens" [**35**, p. 67], adding that

> We are in a better position, because Euler, in the years between 1742 and 1747, constructed a proof precisely of that kind; it is such that we may with some verisimilitude attribute its substance to Fermat.

Weil proceeds to sketch Euler's proof.

The problem about sums of two squares is one of the first topics Fermat studied, and it led him to other important results, for example, that

(a) Every prime of the form $8n + 1$ or $8n + 3$ can be written as $x^2 + 2y^2$;

(b) Every prime of the form $3n + 1$ can be written as $x^2 + 3y^2$; and

(c) Every integer is a sum of four squares.

Other related questions he considered are cited by Weil [**35**, pp. 59–61, 69–75, 80–92].

A look ahead The above results were extended in various directions in subsequent centuries:

(i) *Sums of kth powers* Fermat was proud to have shown that every integer is a sum of four squares, noting Descartes' failure to do so [**25**, p. 346]. The proposition was probably already known to Diophantus and was formally conjectured by Bachet. Euler was captivated by this result and tried for many years to prove it, without success. It was left to Lagrange to give a proof (in 1770).

A natural question suggested itself: Is every integer a sum of kth powers? Waring stated (in 1782) that every integer is a sum of nine cubes, nineteen 4th powers, "and so on" [**19**, p. 297]. The following came to be known as Waring's Problem: Given a positive integer k, does the equation $n = x_1^k + x_2^k + \cdots + x_s^k$ hold for every integer n, where s depends on k but not on n? If so, what is the smallest value of s for a given k (usually denoted by $g(k)$)?

Waring's Problem was solved only in 1909, by Hilbert, who proved the *existence* of s for each k without determining the value of $g(k)$ for various k. Before that time the value of $g(k)$ was known to exist only for about half a dozen values of k. In particular, it was known that $g(3) = 9$ and $g(4) = 19$, so Waring's statement turned out to have been correct [**12**]. It is now known that $g(k) = 2^k + [(3/2)^k] - 2$, provided that $2^k\{(3/2)^k\} + [(3/2)^k] \leq 2^k$, where for any real number x, $[x]$ denotes the greatest integer not exceeding x, and $\{x\} = x - [x]$. A similar result holds when the above inequality fails [**34**, p. 301]. However, this is not the end of the story as far as Waring's Problem is concerned. A recent survey article by Vaughan and Wooley includes a bib-

liography of 162 items [**34**]. Hardy and Wright [**19**] devote an entire chapter to the classical theory.

Much work has also been done since Fermat's time on the representation of integers as sums of *squares*. For example, which integers are sums of *three* squares? Can the above results on sums of squares be extended to algebraic integers? Some of this work is very subtle and related to Artin and Schreier's work in the 1920s on formally real fields. (A field is *formally real* if -1 cannot be represented as a sum of squares of elements in the field.) Artin used the theory of formally real fields to solve Hilbert's 17th Problem, posed at the International Congress of Mathematicians in Paris in 1900, which says that every positive definite rational function in n variables over the reals is a sum of squares of rational functions. A recent book by Yandell is devoted to Hilbert's Problems [**37**].

(ii) *Primes of the form* $x^2 + ny^2$ Euler proved Fermat's results about the representation of primes in the form $x^2 + ny^2$ for $n = 1$, 2, and 3, but he already had difficulty with the case $n = 5$, essentially because the class number of the quadratic forms $x^2 + y^2$, $x^2 + 2y^2$, and $x^2 + 3y^2$ is 1, while that of $x^2 + 5y^2$ is 2 [**11**; **13**, p. 18]. (Fermat, too, realized that the case $n = 5$ was different from those for which $n = 1$, 2, and 3 [**13**, p. 18].) However, studying problems about the representation of primes in the form $x^2 + ny^2$ led Euler to conjecture the *quadratic reciprocity law*, the relationship between the solvability of $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ [**1**]. This is so because of the following result: $p \mid x^2 + ny^2$ and $(x, y) = 1$ if and only if $z^2 \equiv -n \pmod{p}$ has a solution; that is, $-n$ is a quadratic residue (mod p) [**11**, p. 13].

The problem of representing primes in the form $x^2 + ny^2$ for arbitrary n is very difficult, and was solved only in the 20th century using high-powered tools of class field theory. It is the subject of an entire book by Cox [**11**].

(iii) *Binary quadratic forms* A binary quadratic form is an expression of the type $ax^2 + bxy + cy^2$, with a, b, and c integers. The question of the representation of integers by binary quadratic forms, namely, given a fixed form $ax^2 + bxy + cy^2$, determining the integers n such that $n = ax^2 + bxy + cy^2$ for some x and y, became one of the central topics in number theory, studied intensively by Lagrange and treated masterfully by Gauss in his *Disquisitiones Arithmeticae*. This was an outgrowth of the investigations of Fermat and Euler as outlined above [**1, 17, 35**].

Fermat's Last Theorem (FLT)

> It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvellous demonstration of this proposition, which this margin is too narrow to contain [**13**, p. 2].

This is Fermat's famous note, written, perhaps in the 1630s, in the margin of Bachet's translation of Diophantus' *Arithmetica* alongside his Problem II.8, which asks "to divide a given square into two squares" [**20**, p. 144]. Symbolically, it says that $z^n = x^n + y^n$ has no positive integer solutions if $n > 2$. This came to be known as Fermat's Last Theorem. (As we mentioned, Fermat made many assertions in number theory without proof; all but one were later proved by Euler, Lagrange, and others. The exception—the last unproved "result"—was presumably the reason for the name "Fermat's Last Theorem." Of course, we now have a proof of that too.)

Fermat never published his "marvellous demonstration," and some very prominent mathematicians, among them Weil and Wiles, believe that he was probably mistaken in thinking he had a proof, and that perhaps he later realized this [**28**, pp. 74–75; **35**, p. 104]. For, it was only in the margin of Diophantus' *Arithmetica* that Fermat claimed to have proved FLT for arbitrary n. In later correspondence on this problem, he referred only to his having proofs of the theorem for $n = 3$ and $n = 4$. (This was discussed in a recent article by Fogarty and O'Sullivan in the MAGAZINE [**16**].) As Weil put it [**35**, p. 104]:

> For a brief moment perhaps, and perhaps in his younger days, he must have deluded himself into thinking that he had the principle of a general proof; what he had in mind on that day can never be known.

Fermat's only published proof in number theory was of a proposition whose immediate corollary is a proof of FLT for $n = 4$. The proposition in question states that the area of a right-angled triangle (with integer sides) cannot be a square (of an integer), that is, if $x^2 + y^2 = z^2$ for integers x, y, z, then there is no integer u such that $xy/2 = u^2$. This problem was inspired by those in Diophantus' *Arithmetica*, Book VI, each of whose 26 problems asks for a right-angled triangle satisfying given conditions. Fermat's proof was found by his son, Samuel, in the margin of Fermat's copy of the *Arithmetica*, and was included in his *Observations on Diophantus* (Observation 45), posthumously published by Samuel. The proof is ambiguous in places, but Fermat noted that "The margin is too small to enable me to give the proof completely and with all detail"(!) [**13**, p. 12].

In the proof just mentioned, Fermat introduced the *method of infinite descent*. That is, assuming that there exists some positive integer u satisfying the above conditions, he showed that there is a positive integer $v < u$ satisfying the same conditions. Repeating this process ad infinitum clearly leads to a contradiction. Fermat was very proud of his method of infinite descent, using it (he said) in the proofs of many of his number-theoretic propositions. He predicted that "this method will enable extraordinary developments to be made in the theory of numbers" [**20**, p. 293]. In an account of his number-theoretic work sent to Huygens in 1659, he gave more details [**35**, p. 75]:

> As ordinary methods, such as found in the books, are inadequate to proving such difficult propositions, I discovered at last a most singular method ... which I called *infinite descent*. At first I used it only to prove negative assertions, such as ... "there is no right-angled triangle of numbers whose area is a square." ... To apply it to affirmative questions is much harder, so that, when I had to prove that "Every prime of the form $4n + 1$ is a sum of two squares," I found myself in a sorry plight. But at last such questions proved amenable to my method ...."

A look ahead Fermat's method of infinite descent is logically only a variant of the Principle of Mathematical Induction, but it provided Fermat, and indeed his successors, with a powerful tool for proving number-theoretic results. The method of infinite descent may be likened, conceptually, to Dirichlet's pigeonhole principle: both are mathematically trivial observations with far-reaching ramifications.

In the 18th century, FLT was proved for only one exponent, $n = 3$—by Euler, using the method of infinite descent (there was, however, a gap in his proof). In fact, the method of infinite descent was used in all subsequent proofs of FLT, for various values of the exponent n. In the 19th century, attempts to prove FLT motivated the introduction of ideal numbers by Kummer, and later of ideals by Dedekind, giving rise also to

such fundamental algebraic concepts as ring, field, prime ideal, unique factorization domain, and Dedekind domain. These developments led, in the hands of Dedekind and Kronecker, to the founding in the 1870s of *algebraic number theory*, the marriage of number theory and abstract algebra. In the 20th century, FLT entered the mainstream of mathematics by becoming linked with a profound mathematical problem, the Shimura-Taniyama Conjecture, which says that every elliptic curve is modular. This, in turn, led to Wiles' 1994 proof of FLT, using deep ideas from various branches of mathematics [**24**].

Bachet's equation and Pell's equation

The two equations are, respectively,

$$x^2 + k = y^3 \quad \text{(with } k \text{ any integer)} \quad \text{and} \quad x^2 - dy^2 = 1$$

(with d a nonsquare positive integer). These equations, along with the Pythagorean equation $x^2 + y^2 = z^2$ and the Fermat equation $x^n + y^n = z^n$, $n > 2$, are perhaps the most important Diophantine equations. Fermat studied all of the above.

(a) Bachet's equation A special case of the Bachet equation, $x^2 + 2 = y^3$, appears in Diophantus' *Arithmetica* (Problem VI.17). He wants "To find a right-angled triangle such that the area added to the hypotenuse gives a square, while the perimeter is a cube." In the course of solving it, he reduces the problem, saying that "Therefore we must find some square which, when 2 is added to it, becomes a cube" [**20**, p. 241]. The equation $x^2 + k = y^3$ was considered by Bachet, who raised the question of its solvability.

Fermat gave the solution $x = 5$, $y = 3$ for $x^2 + 2 = y^3$ and, for $x^2 + 4 = y^3$, the solutions $x = 2$, $y = 2$, and $x = 11$, $y = 5$. In both cases he used infinite descent, he claims. Of course it is easy to see that these are solutions of the respective equations, but it is rather difficult to verify that they are the *only* (positive) solutions, which is what Fermat had in mind. He challenged his colleagues to confirm these results: "I don't know," he wrote, "what the English will say of these negative propositions or if they will find them too daring. I await their solution and that of M. Frenicle..." [**25**, p. 343].

Frenicle "could hardly believe" Fermat's claims, which he "found too daring and too general" [**25**, p. 343]. As for the English, Wallis responded (via Digby, to whom Fermat had sent his letter) as follows [**25**, p. 345]:

> I say... [about] his recent negative propositions... [that] I am not particularly worried whether they are true or not, since I do not see what great consequence can depend on their being so. Hence, I will not apply myself to investigating them. In any case, I do not see why he displays them as something of a surprising boldness that should stupefy either M. Frenicle or the English; for such negative conditions are very common and very familiar to us.

Mahoney has the following take on this [**25**, p. 345]:

> Wallis' overwhelming sense that number theory consisted essentially of wearying computations closed his mind to the promises Fermat was making about the new arithmetic.

A look ahead Mordell noted that "[The Bachet equation $x^2 + k = y^3$] has played a fundamental role in the development of number theory" [**27**, p. 238]. It has been studied for the past 300 years. Special cases were solved by various mathematicians throughout the 18th and 19th centuries. Euler introduced a fundamental new idea to solve $x^2 + 2 = y^3$ by factoring its left-hand side, which yielded the equation $(x + \sqrt{2}i)(x - \sqrt{2}i) = y^3$. The result was an equation in a domain D of "complex integers," where $D = \{a + b\sqrt{2}i : a, b \in Z\}$. This was the first use of complex numbers—"foreign objects"—in number theory. The ideas involved whether D is a unique factorization domain, and were part of the development that gave rise in the 19th century to algebraic number theory. Books by Adams and Goldstein [**1**] and Ireland and Rosen [**23**] discuss aspects of these issues. (See also the previous section.)

In the 1920s Mordell showed that $x^2 + k = y^3$ has finitely many (integer) solutions for each k (it may have none; for example, $x^2 - 45 = y^3$ [**27**, p. 239]), and in the 1960s Baker and Stark gave explicit bounds for x and y in terms of k, so that in theory all solutions for a given k can be found by computation. Moreover, Baker notes that "techniques have been devised which, for a wide range of numerical examples, render the problem of determining the complete list of solutions in question accessible to machine computation" [**4**, p. 45].

It should be pointed out that Bachet's equation is an important example of an elliptic curve. (An *elliptic curve* is a plane curve represented by the equation $y^2 = ax^3 + bx^2 + cx + d$, where a, b, c, d are integers or rational numbers, and the cubic polynomial on the right side of the equation has distinct roots.) In fact, "[the Bachet equation], special as it may seem, is a central player in the Diophantine drama and in a certain sense 'stands for' the arithmetic theory of elliptic curves." This comment comes from an article by Mazur, who adds that "One of the objects of this article is to give hints about why the [Bachet] equation plays this central role" [**26**, p. 196].

Fermat dealt with many Diophantine equations, all, except for the Fermat equation $x^n + y^n = z^n$, of genus 0 or 1 [**35**, p. 104]. (For a sufficiently smooth curve given by a polynomial equation of degree n, the genus is $(n - 1)(n - 2)/2$; see also [**7**, p. 13].) Most of these define elliptic curves—algebraic curves of genus 1. The study of elliptic curves has involved the use of powerful methods, including those of algebraic geometry [**7, 23, 26, 27**]. "The theory of elliptic curves, and its generalization to curves of higher genus and to abelian varieties," notes Weil, "has been one of the main topics in modern number theory. Fermat's name, and his method of infinite descent, are indissolubly bound with it; they promise to remain so in the future" [**35**, p. 124].

(b) Pell's equation Pell's equation, $x^2 - dy^2 = 1$, was known throughout the ancient world [**12**]. (The equation was inappropriately named by Euler after the British mathematician John Pell.) Special cases were considered by the Greeks, and the Indians of the Middle Ages had a procedure for solving the general case, as did British mathematicians of the 17th century [**35**].

Weil asserts that "the study of the [quadratic] form $x^2 - 2y^2$ must have convinced Fermat of the paramount importance of the equation $x^2 - Ny^2 = \pm 1$" [**35**, p. 92]. (The equation $x^2 - dy^2 = -1$ is also sometimes known as Pell's equation.) Edwards counters that "it is impossible to reconstruct the way in which Fermat was led to this problem" [**13**, p. 27].

Fermat challenged mathematicians to show that Pell's equation has infinitely many solutions for each d. This is how he phrased it [**20**, p. 286]:

> Given any number whatever that is not a square, there are also given an infinite number of squares such that, if the square is multiplied into the given number and unity is added to the product, the result is a square.

He was aware of Brouncker's and Wallis' solutions of Pell's equation, but found them wanting, lacking a "general demonstration" [**25**, p. 328]. What he had in mind is a proof that the equation always has a solution, in fact, infinitely many solutions, and that the known methods of finding solutions yield all of them. Fermat declared that he had such a demonstration, though he did not divulge it, other than to indicate that it involved his method of infinite descent [**25**, p. 350]. He also employed a "method of ascent" to obtain new solutions from given ones [**35**, pp. 105 and 112].

Fermat challenged Frenicle to solve the equation $x^2 - 61y^2 = 1$. "He must have known, of course, that the smallest solution [of this equation is]

$$(1766319049, 226153980),"$$

says Weil [**35**, p. 97]. There is no discernible pattern to the sizes of the minimal solutions of Pell's equation. For example, the minimal solution of $x^2 - 75y^2 = 1$ is (26, 3). (The minimal solution of Pell's equation, the so-called "fundamental solution," is one in terms of which all others can be expressed [**1**].)

A look ahead The definitive treatment of Pell's equation was given by Lagrange in the latter part of the 18th century. He was the first to prove that it has a solution for every nonsquare positive integer d, and to give a procedure for finding all solutions for a given d by means of the continued fraction expansion of $\sqrt{d}$—another use of "foreign objects" in number theory. There are, indeed, infinitely many solutions for each d [**6, 17**].

Pell's equation has continued to play an important role in number theory. For example:

(i) It is a key to the solution of arbitrary quadratic Diophantine equations, as well as other Diophantine equations [**27**].

(ii) Its solutions yield the best approximation (in some sense) to $\sqrt{d}$. (Pell's equation $x^2 - dy^2 = 1$ can be written as $(x/y)^2 = d + 1/y^2$, so that for large y, x/y is an approximation to $\sqrt{d}$. This may already have been realized by the Greeks [**6, 12, 31**].)

(iii) There is a 1-1 correspondence between the solutions of $x^2 - dy^2 = 1$ and the invertible elements of the domain of integers of the quadratic field $Q(\sqrt{d}) = \{s + t\sqrt{d} : s, t \text{ rational}\}$ [**1, 36**].

(iv) The equation played a crucial role in the solution (in 1970) of Hilbert's 10th Problem, the nonexistence of an algorithm for solving arbitrary Diophantine equations [**37**].

For these and other reasons, the Pell equation has been studied extensively, but much remains to be done [**36**, p. 428]:

> The current state of the art in solving the Pell equation [computationally] is far from satisfactory. In spite of the enormous progress that has been made on this problem in the last few decades, we are still without answers to many fundamental questions. However, we are, it seems, beginning to understand what the questions should be.

Conclusion

We have considered only some of Fermat's contributions to number theory. These comprise results, methods, and concepts not seriously considered (if at all) before Fer-

mat. Moreover, they turned out to have applications in various number-theoretic contexts and became harbingers of significant departures in number theory in succeeding centuries. Without doubt, these accomplishments entitle Fermat to be known as the founder of modern number theory.

In 1659 Fermat wrote a four-page letter to Carcavi, intended for Huygens, which he titled "An account of new discoveries in the science of numbers," and in which he meant to give a brief summary of some of his accomplishments in number theory. We conclude with his reflections, taken from the last paragraph [**25**, p. 351]:

> Perhaps posterity will thank me for having shown it that the ancients did not know everything, and this account will pass into the mind of those who come after me as a "passing of the torch to the next generation."

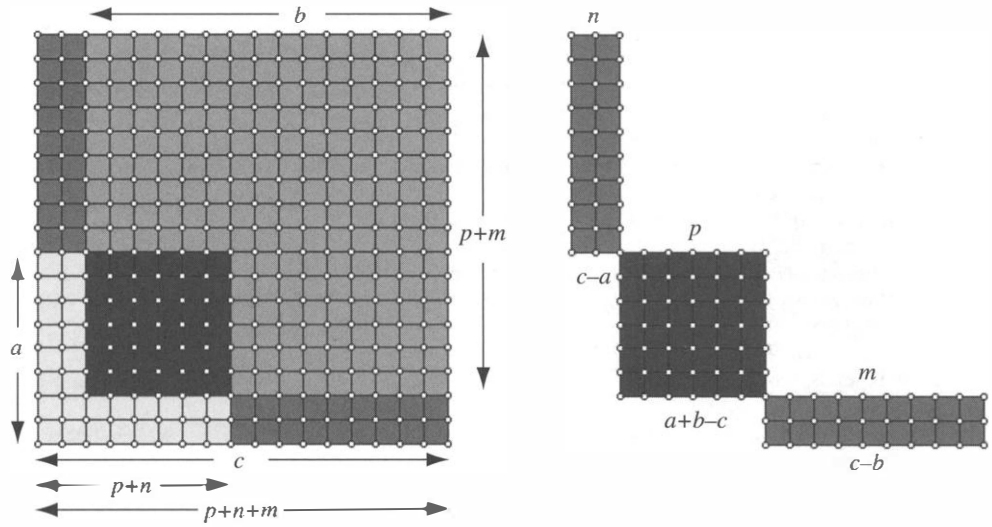
REFERENCES

1. W. W. Adams and L. J. Goldstein, *Introduction to Number Theory*, Prentice-Hall, Englewood Cliffs, NJ, 1976.
2. A. G. Agargün and E. M. Özkan, A historical survey of the Fundamental Theorem of Arithmetic, *Hist. Math.* **28** (2001), 207–214.
3. E. Bach and J. Shallit, *Algorithmic Number Theory*, Vol. 1, MIT Press, Cambridge, MA, 1996.
4. A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, Cambridge, UK, 1990.
5. K. Barner, How old did Fermat become?, *NTM, Intern. Jour. Hist. and Ethics of Natur. Sc., Techn. and Med.* **8** (4), October 2001.
6. E. J. Barbeau, *Pell's Equation*, Springer, New York, 2003.
7. I. G. Bashmakova, *Diophantus and Diophantine Equations*, Mathematical Association of America, 1997. (Translated from the Russian by A. Shenitzer.)
8. E. T. Bell, *Men of Mathematics*, Simon and Schuster, New York, 1937.
9. F. Bornemann, PRIMES is in P: A breakthrough for 'everyman', *AMS Notices* **50** (2003), 545–552.
10. D. M. Bressoud, *Factorization and Primality Testing*, Springer, New York, 1989.
11. D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, New York, 1989.
12. L. E. Dickson, *History of the Theory of Numbers*, 3 vols., Chelsea, New York, 1966.
13. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer, New York, 1977.
14. C. R. Fletcher, A reconstruction of the Frenicle-Fermat correspondence, *Hist. Math.* **18** (1991), 344–351.
15. C. R. Fletcher, Fermat's theorem, *Hist. Math.* **16** (1989), 149–153.
16. K. Fogarty and C. O'Sullivan, Arithmetic progressions with three parts in prescribed ratio and a challenge of Fermat, this MAGAZINE **77** (2004), 283–292.
17. J. R. Goldman, *The Queen of Mathematics: A Historically Motivated Guide to Number Theory*, A. K. Peters, Natick, MA, 1998.
18. E. Grosswald, *Representation of Integers as Sums of Squares*, Springer, New York, 1985.
19. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, London, 1959.
20. T. L. Heath, *Diophantus of Alexandria: A Study in the History of Greek Algebra*, 2nd ed., Dover, New York, 1964. Contains a translation into English of Diophantus' *Arithmetica*, a 130-page Introduction to Diophantus' and related work, and a 60-page Supplement on Fermat's number-theoretic work.
21. T. L. Heath (ed.), *The Thirteen Books of Euclid's Elements*, 3 vols., 2nd ed., Dover, New York, 1956.
22. K. Iga, A dynamical systems proof of Fermat's little theorem, this MAGAZINE **76** (2003), 48–51.
23. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.
24. I. Kleiner, From Fermat to Wiles: Fermat's Last Theorem becomes a theorem, *Elem. Math.* **55** (2000), 19–37.
25. M. S. Mahoney, *The Mathematical Career of Pierre de Fermat*, 2nd ed., Princeton Univ. Press, Princeton, 1994.
26. B. Mazur, Questions about powers of numbers, *AMS Notices* **47** (2000), 195–202.
27. L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.
28. C. J. Mozzochi, *The Fermat Diary*, American Mathematical Society, 2000.
29. H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhäuser, Boston, 1994.
30. W. Scharlau and H. Opolka, *From Fermat to Minkowski: Lectures on the Theory of Numbers and its Historical Development*, Springer, New York, 1985.
31. J. Stillwell, *Elements of Number Theory*, Springer, New York, 2003.

32. ———, *Mathematics and its History*, 2nd ed., Springer, New York, 2002.
33. P. Tannery and Ch. Henry (eds.), *Oeuvres de Fermat*, 4 vols., Gauthier-Villars, Paris, 1891–1912, and a *Supplément*, ed. by C. de Waard, Paris, 1922.
34. R. C. Vaughan and T. D. Wooley, Waring's problem: a survey. In *Number Theory for the Millennium III*, ed. by M. A. Bennett, et al., A. K. Peters, Natick, MA, 2002, 301–340.
35. A. Weil, *Number Theory: An Approach through History, from Hammurapi to Legendre*, Birkhäuser, Boston, 1984.
36. H. C. Williams, Solving the Pell equation. In *Number Theory for the Millennium III*, ed. by M. A. Bennett, et al., A. K. Peters, Natick, MA, 2002, 397–435.
37. B. H. Yandell, *The Honors Class: Hilbert's Problems and their Solvers*, A K Peters, Natick (Mass), 2002.

Proof Without Words: Pythagorean Triples and Factorizations of Even Squares

There is a one to one correspondence between Pythagorean triples and factorizations of even squares of the form $p^2 = 2nm$.



If $a^2 + b^2 = c^2$, then $(a + b - c)^2 = 2(c - a)(c - b)$.

If $p^2 = 2nm$, then $(p + n)^2 + (p + m)^2 = (p + n + m)^2$.

—JOSÉ GOMEZ
SOUTH JUNIOR HIGH SCHOOL
NEWBURGH NY 12550

EDITOR'S NOTE: Author Darryl McCullough, whose article *Height and Excess of Pythagorean Triples* appears in this issue, points out that another way to see the correspondence between factorizations of even integers and Pythagorean triples is through $\langle e, h\rangle$-coordinates: In the notation of his article, each factorization $p^2 = 2mn$ corresponds to the two pairs $\langle p, m\rangle$ and $\langle p, n\rangle$, which represent a Pythagorean triangle and its mirror image.

The Singled Out Game

KENNAN SHELTON
Rhodes College
Memphis, TN 38112
shelton@rhodes.edu

In the mid 1990s, the cable music video channel MTV produced *Singled Out*, a game show in which fifty men competed to win a date with a single woman (for gender equity, the second half of the show featured fifty women vying for one man). Through a series of elimination stages—most of them embarrassing to the contestants—the field of potential suitors was reduced to only three.

To determine the winner from the final three contestants, the woman was presented with a series of either/or questions. Each man attempted to guess the woman's answer and those who guessed correctly took one step toward the woman. The winner was the man to take five steps and reach the woman. (A tie-breaker round was used if necessary.) Much of the time the men seemed to have no idea what answers the woman chose. I myself had no clue what she might answer—it seemed to me that she was simply flipping a coin to make her decision.

The interesting feature of the show was how the men announced their guesses. They were arranged in a fixed order and each in turn announced his guess so that the others could hear. Thus it was possible for the second and third men to modify their choices based on what the previous announcements had been. This raises the question: do the second and third men have any advantage, even if no man has any clue what the woman might answer? If so, what strategy could he employ to exploit this advantage? Would a little knowledge of mathematics help him to win?

The Singled Out game described in this article is an abstraction of the final stage of the MTV game show:

> *The Singled Out Game.* The Singled Out game is played in a series of rounds. In each round, a coin is flipped and the result is kept secret. Each player, one at a time, announces his guess so that the other players hear it. The order in which the players announce their guesses is determined at the start of the game and remains fixed throughout. After all players have guessed, the coin is revealed and all players who guessed correctly earn one point; incorrect guesses earn no points. The game continues until a player reaches n points and is declared the winner. If there is a tie, the winner is determined by a random selection from among those who tied.

In this paper we investigate the Singled Out game with two and three players. For the two-player game, the second player does indeed have an advantage—we obtain an expression for the probability that the second player wins and show that this probability approaches 1 as n approaches infinity. We then look at what happens if the first player is a good guesser (he is correct with some probability greater than $1/2$) and show that this gives him at least a constant nonzero chance of winning, no matter how many points are needed to win. Finally, we look at the three-player game and present experimental evidence that the third player does have an advantage, though his strategy is counter-intuitive.

The analysis of the two-player Singled Out game involves *Catalan numbers*, a well-known sequence, which we briefly describe here. Catalan numbers may be used to enumerate a wide variety of objects. Euler first described them in the 18th century

when he investigated the number of triangulations of convex polygons; Catalan used them one hundred years later to count the number of binary parenthesizations of a string. Over 60 applications of Catalan numbers are given in [**5**]. For more information about Catalan numbers, including an extensive bibliography, see [**3**]. In this paper we will focus on one application of Catalan numbers: the enumeration of *ballot paths*.

In a two-dimensional integer lattice, consider the paths from $(0, 0)$ to (n, k), $n \geq k \geq 0$, that move either horizontally to the right or vertically up by one-unit steps. Ballot paths are those paths that never rise above the diagonal, that is, for all (a, b) in the path, we have $a \geq b$. For example, there are 5 ballot paths from $(0, 0)$ to $(3, 3)$ (see FIGURE 1).

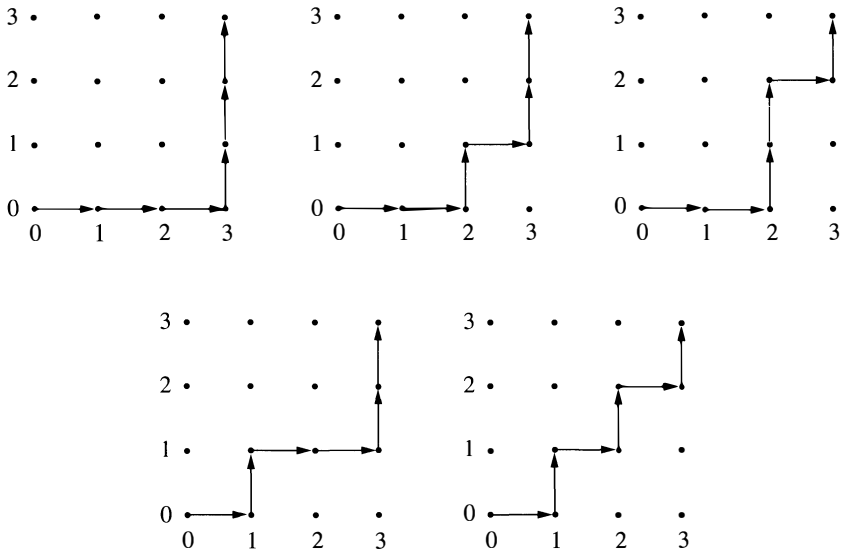


Figure 1 The five ballot paths to (3, 3)

The term "ballot path" comes from the role these paths play in solving the *Ballot Problem*. Suppose that candidates A and B receive n and k votes respectively, with $n \geq k$. The Ballot Problem asks for the probability that, as we count the ballots, A is never behind B in the tally. This is equivalent to asking what proportion of all paths from $(0, 0)$ to (n, k) are ballot paths. The Ballot Problem was originally solved by Bertrand; an elegant solution was given by André using what is now referred to as André's Reflection Principle [**1**]. We should note that the original problem considered by Bertrand and André asked for the probability that the count for A is *always ahead* of B (this probability is $(n-k)/(n+k)$). For our purposes, however, it is more convenient to allow A and B to tie during the tally.

Let $C(n, k)$ denote the number of ballot paths from $(0, 0)$ to (n, k), $n \geq k \geq 0$. It is easy to see that the $C(n, k)$ satisfy the recurrence equations:

$$\begin{aligned} C(n,k) &= C(n-1,k) + C(n,k-1), && n > k \geq 1; \\ C(n,n) &= C(n,n-1), && n \geq 1; \\ C(n,0) &= 1, && n \geq 0. \end{aligned}$$

The reader is invited to show that $C(n, k)$ has the closed form expression

$$C(n,k) = \binom{n+k}{k} - \binom{n+k}{k-1}. \tag{1}$$

The nth Catalan number, C_n, is the number of ballot paths from (0, 0) to (n, n), i.e., $C_n = C(n, n)$. The first several Catalan numbers are 1, 1, 2, 5, 14, and 42. Using (1) we see that

$$C_n = \frac{1}{n+1}\binom{2n}{n}. \tag{2}$$

A recurrence relation and an alternative expression for C_n will also be useful to us. These can be derived easily from (2).

$$C_n = \frac{2(2n-1)}{n+1}C_{n-1}, \quad C_0 = 1; \tag{3}$$

$$C_n = \frac{2^n}{(n+1)!}\prod_{k=1}^{n}(2k-1) = \frac{4^n}{(n+1)!}\prod_{k=1}^{n}(k-1/2), \quad n \geq 1. \tag{4}$$

Two-player Singled Out

Suppose that we only have two players, Adam and Barry, who are playing to n points and that Adam always guesses first. We will assume in this section that Adam, having no information at all, has probability $1/2$ of guessing correctly. Barry, on the other hand, does have some information: he knows what Adam has guessed. We will see that this extra piece of information is enough to give Barry the edge with the right strategy.

A play of the game may be represented as a *game path* on a two-dimensional integer lattice. The integer point (a, b), $0 \leq a, b$, represents the game state in which Adam has a points and Barry has b points. Then a game to n points can be represented as a path from (0, 0) to one of the points (n, k) or (k, n) for $0 \leq k \leq n$. Note that if $k = n$ then the game ends in a tie and the winner is decided randomly.

Since the players will either gain a point or not, a path from (0, 0) to a winning state will move in one of three nontrivial ways: *right* if Adam guesses correctly and Barry guesses incorrectly, *up* if Adam guesses incorrectly and Barry guesses correctly, and *diagonally* if Adam and Barry both guess correctly. In the case that both Adam and Barry guess incorrectly, the game state remains the same. An example game path is presented in FIGURE 2, where Adam has won with 6 points versus 5 points for Barry.

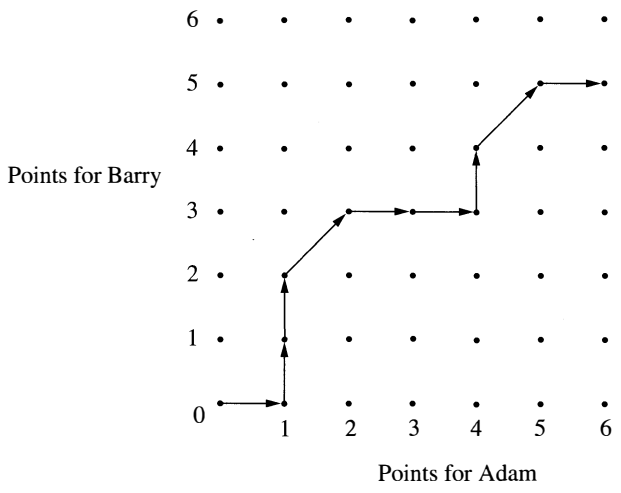


Figure 2 A winning game path for Adam

Two simple strategies that Barry may employ are the *copy-cat* strategy (always make the same guess as Adam) and the *contrarian* strategy (always make the opposite guess as Adam). However, it is not hard to show that either of these strategies will give Barry a probability of $1/2$ of winning. Thus they confer no advantage to Barry.

But Barry can actually increase his probability of winning to greater than $1/2$ by the following strategy:

> *Contrari-cat strategy*: Whenever Barry is behind or tied with Adam, he should choose the opposite of Adam. Whenever Barry is ahead of Adam, he should choose the same as Adam.

Using the contrari-cat strategy, if Barry ever gets ahead of Adam then Barry will be guaranteed to win as he will always be one point ahead of Adam. The probability that Barry gets ahead on the first flip of the coin (and then wins the game) is $1/2$, so this strategy is at least as good as the copy-cat and contrarian strategies. If they are playing to only one point then Barry cannot do any better.

However, if the game requires two or more points to win, Barry will have a nonzero probability of catching up to Adam and then getting ahead. Thus the probability that Barry wins is greater than $1/2$ and he has the advantage. For example, suppose that the game is being played to 3 points. For Barry to win using the contrari-cat strategy, one of the following situations must occur:

1. Barry gets ahead on the first flip (from (0, 0) to (0, 1))
2. Barry loses the first flip, but catches up on the second and gets ahead on the third (from (1, 1) to (1, 2))
3. Barry loses two flips (the first two or the first and third) but then catches up and gets ahead on the fifth flip (from (2, 2) to (2, 3)).

The possible game paths are shown in FIGURE 3. Note that there are two winning game paths passing through (2, 2), each with equal probability (1/32) of occurring. Thus the probability that Barry wins will be $1/2 + 1/8 + 2/32 = 11/16$.

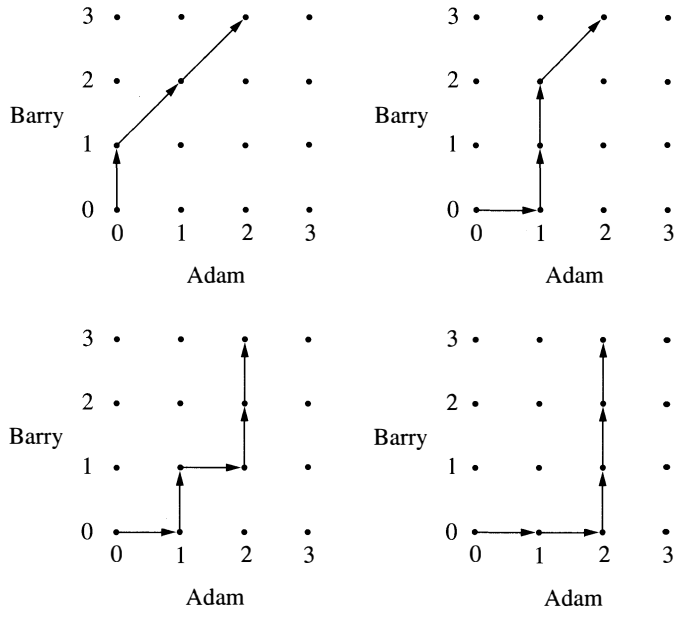


Figure 3 Barry's winning game paths to 3 points

We want to determine the probability $P_B(n)$ that Barry wins when playing to n points using the contrari-cat strategy. In general, Barry will win if at any time the game path crosses above the diagonal from (0, 0) to (n, n), since he will be ahead at this point and his strategy will prevent Adam from winning. Thus winning game paths are in one-to-one correspondence with the set of ballot paths from $(0, 0)$ to (k, k), $0 \le k \le n-1$.

Suppose G is a winning game path for Barry that first crosses above the diagonal at (k, k) for some k between 0 and $n-1$. The path G must contain k moves to the right and k moves up, followed by one more move up (to cross the diagonal). All moves occur with probability $1/2$, so the probability that G occurs is $1/(2 \cdot 4^k)$. However, there are C_k such paths, so the probability that Barry wins by crossing at (k, k) is $C_k/(2 \cdot 4^k)$. Therefore

$$P_B(n) = \frac{1}{2} \sum_{k=0}^{n-1} \frac{1}{4^k} C_k.$$

Since this formula shows that $P_B(n+1) > P_B(n)$, as the number of points required to win the game increases, Barry has a better and better chance of winning when using the contrari-cat strategy. We can use this fact to show that the contrari-cat strategy is better than any other. For clearly if Barry is ahead then he should follow the copycat strategy and if he is behind then he should follow the contrarian strategy (in order to win, Barry must say the opposite of Adam at some point; the earlier he does this, the greater his probability of catching up before Adam wins the game). We only need to determine what Barry should do at the start of the game, when the score is tied. If Barry did not follow the contrarian strategy at this point then the probability that he wins will be the same as if Adam and Barry were playing to one fewer point. But the fact that $P_B(n)$ is a strictly increasing function of n, coupled with a simple induction argument, shows that Barry would be better off playing the contrarian strategy. Thus the contrari-cat strategy is optimal for Barry—no other strategy can guarantee a higher probability of winning.

In fact, as n approaches infinity, $P_B(n)$ approaches 1, as we show next.

THEOREM 1. *As the two-player Singled Out game is played to an increasing number of points, the probability that the second player wins using the contrari-cat strategy approaches* 1, *that is,*

$$\lim_{n \to \infty} P_B(n) = 1.$$

Proof. From the definition of $P_B(n)$, we have that

$$P_B(n) = \frac{1}{2} \sum_{k=0}^{n-1} \frac{1}{4^k} C_k = P_B(n-1) + \frac{1}{2 \cdot 4^{n-1}} C_{n-1}.$$

Using induction, we will first show that for all $n \ge 1$,

$$P_B(n) = 1 - \frac{n+1}{4^n} C_n. \tag{5}$$

Inspection shows that (5) holds when $n = 1$. Suppose that (5) holds for some $n \ge 1$. Using the recursive expression (3) for the Catalan numbers we have

$$P_B(n+1) = P_B(n) + \frac{1}{2 \cdot 4^n} C_n$$
$$= 1 - \frac{n+1}{4^n} C_n + \frac{1}{2 \cdot 4^n} C_n = 1 - \frac{2n+1}{2 \cdot 4^n} C_n$$
$$= 1 - \frac{2n+1}{2 \cdot 4^n} \cdot \frac{n+2}{2(2n+1)} C_{n+1} = 1 - \frac{n+2}{4^{n+1}} C_{n+1},$$

so by induction (5) holds for all $n \geq 1$.

Then, using the alternative expression (4) for C_n, we have

$$P_B(n) = 1 - \frac{n+1}{4^n} \cdot \frac{4^n}{(n+1)!} \prod_{k=1}^{n} (k - 1/2)$$
$$= 1 - \frac{\prod_{k=1}^{n} (k - 1/2)}{\prod_{k=1}^{n} k}$$
$$= 1 - \prod_{k=1}^{n} \left(1 - \frac{1}{2k}\right).$$

Thus to show that $P_B(n)$ approaches 1, it suffices to show that the infinite product

$$\prod_{k=1}^{\infty} \left(1 - \frac{1}{2k}\right) \tag{6}$$

converges to 0. Let $p_n = \prod_{k=1}^{n} (1 - 1/(2k))$. Since $\{p_n\}$ is a decreasing sequence bounded below by 0, it must converge and so (6) exists. The infinite product converges to a nonzero number if and only if the series

$$\sum_{k=1}^{\infty} \ln \left(1 - \frac{1}{2k}\right)$$

converges [**2**, p. 164]. However, using the power series expansion of $\ln(1 - x)$,

$$\ln(1 - x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \cdots \qquad |x| < 1,$$

we see that for $k \geq 1$, $\ln(1 - 1/2k) \leq -1/2k$. Thus the series cannot converge and so (6) converges to 0. Therefore $\lim_{n \to \infty} P_B(n) = 1$. ■

As a corollary to Theorem 1, we have the following identity that will be used later:

$$\sum_{k=0}^{\infty} \frac{1}{4^k} C_k = 2.$$

Remark Alternatively, we might have shown that the probability $P_A(n)$ that Adam wins, converges to 0 as n approaches infinity. Winning paths for Adam are precisely the ballot paths from $(0, 0)$ to (n, k) with $n > k \geq 0$. The reader is invited to use the recurrence properties of $C(n, k)$ to show that

$$P_A(n) = \frac{1}{2^n} \sum_{k=0}^{n-1} \frac{1}{2^k} C(n-1, k)$$

$$= \frac{2n-1}{2n} P_A(n-1)$$
$$= \prod_{k=1}^{n} \left(1 - \frac{1}{2k}\right),$$

which we know converges to 0 as n approaches infinity.

Arbitrary probabilities

In the previous section we assumed that Adam's chance to guess correctly was the same as flipping a fair coin. But what if he is a good guesser? In terms of the MTV game, perhaps Adam has some insight into the psyche of the woman who is answering the questions. Can Adam overcome the advantage Barry has with the contrari-cat strategy? We will show in this section that if Adam has better than even chance to guess correctly, then he will have at least a constant nonzero chance to win, independent of how many points are required. We will assume that Barry has no knowledge of Adam's ability to guess correctly and that he will continue to follow the contrari-cat strategy.

Suppose that Adam is correct with probability $1/2 + t$ for some $t \in [-1/2, 1/2]$ (so he is wrong with probability $1/2 - t$). Barry's contrari-cat strategy will still guarantee a win provided he can get ahead of Adam. But the probability that Barry will get ahead when playing to n points is now a function of t as well as n.

Let $P_B(n, t)$ denote the probability that Barry wins the game when playing to n points and when Adam is correct with probability $1/2 + t$. Thus $P_B(n, 0) = P_B(n)$ as defined in the previous section. Note that $P_B(n, -1/2) = 1$ while $P_B(n, 1/2) = 0$ for all $n \geq 1$. Suppose that $t \in (-1/2, 1/2)$. As before, Barry will win when a game path rises above the diagonal. For each k between 0 and $n-1$, to reach the state (k, k) the game path will need to make k moves to the right and k moves up, followed by one more move up. However, now the probability of a move to the right is $1/2 + t$ while the probability of moving up is $1/2 - t$. Thus

$$P_B(n, t) = \left(\frac{1}{2} - t\right) \sum_{k=0}^{n-1} \left(\frac{1}{2} - t\right)^k \left(\frac{1}{2} + t\right)^k C_k \tag{7}$$

$$= \left(\frac{1}{2} - t\right) \sum_{k=0}^{n-1} \left(\frac{1}{4} - t^2\right)^k C_k. \tag{8}$$

The probability $P_B(n, t)$ is again an increasing function of n for fixed t, because the terms in the sum are positive. Also, $P_B(n, t)$ is a polynomial function of t with $dP_B(n, t)/dt < 0$ so it is a decreasing function of t for fixed n.

We will find an explicit expression for the function $P_B^*(t) = \lim_{n\to\infty} P_B(n, t)$. Note that for $t \leq 0$, it is clear that $P_B^*(t) = 1$ since $P_B(n, t) \geq P_B(n, 0)$ for each $n \geq 1$ and $P_B(n, 0) = P_B(n) \to 1$ by Theorem 1.

For $t \in [-1/2, 1/2]$, set

$$S(t) = \begin{cases} 1 & \text{if } t = \pm 1/2 \\ \displaystyle\sum_{k=0}^{\infty} \left(\frac{1}{4} - t^2\right)^k C_k & \text{otherwise.} \end{cases}$$

Note that $S(t) = S(-t)$ and $S(0) = \sum_{k=0}^{\infty} C_k/4^k = 2$. Since $0 \leq (1/4 - t^2)^k \leq 1/4^k$ for all $k \geq 1$, $S(t)$ exists and is at most 2. Further, $P_B^*(t) = (1/2 - t)S(t)$.

Now, for $t \in [-1/2, 0]$, $P_B^*(t) = 1$ so $S(t) = 2/(1-2t)$. Then $S(t) = 2/(1+2t)$ for $t \in (0, 1/2]$. Therefore

$$P_B^*(t) = \begin{cases} 1 & \text{if } -1/2 \le t \le 0 \\ \dfrac{1-2t}{1+2t} & \text{if } 0 < t \le 1/2. \end{cases}$$

Thus for $t > 0$, the probability that Adam wins is at least $1 - (1-2t)/(1+2t) = 4t/(1+2t)$, for all values of n.

Note that $4t/(1+2t) = 1/2$ when $t = 1/6$. So for large n, for Adam to have an approximately even chance of winning against Barry (who is assumed to be using the contrari-cat strategy), he will need to guess correctly at least $1/2 + 1/6 = 2/3$ of the time.

Three-player Singled Out

We now turn to experimental results for the three-player game, with players Adam, Barry, and Carl. As with the original two-player game, Adam has no information—his probability of guessing correctly is $1/2$. Barry has the same information as before (Adam's choice) and Carl has the most information available to him before he makes his choice (Adam's and Barry's choices).

In this section, we will represent the game states as 3-tuples (a, b, c) where Adam needs a more points to win, Barry needs b more points and Carl needs c more points. The game ends when at least one of a, b, or c is zero. Recall that if there is a tie then we will choose randomly to determine the winner.

Let $P(a, b, c)$ be the 3-tuple denoting the probabilities that Adam, Barry, and Carl (respectively) will win when starting in game state (a, b, c). We will determine $P(a, b, c)$ recursively using the initial values shown in TABLE 1.

TABLE 1: Initial winning probabilities

(a, b, c)	$P(a, b, c)$	(a, b, c)	$P(a, b, c)$
(0, 0, 0)	(1/3, 1/3, 1/3)	(1, 0, 0)	(0, 1/2, 1/2)
(0, 0, 1)	(1/2, 1/2, 0)	(1, 0, 1)	(0, 1, 0)
(0, 1, 0)	(1/2, 0, 1/2)	(1, 1, 0)	(0, 0, 1)
(0, 1, 1)	(1, 0, 0)		

To calculate $P(1, 1, 1)$ we first determine the possible game state outcomes when starting from state (1, 1, 1). Since Adam has an even chance of winning a point no matter what he guesses, we focus on the choices of Barry and Carl. Each has two choices: to say the same as Adam (A) or not ($\neg A$). Since Adam is either correct or incorrect, there are 8 possible outcomes, summarized in TABLE 2. In each entry, the upper 3-tuple is the resulting outcome game state if Adam is correct; the lower 3-tuple is the outcome state if Adam is incorrect. We can then calculate the winning probabilities $P(1, 1, 1)$, shown in TABLE 3.

If Barry chooses A then Carl will certainly choose $\neg A$ as it gives him the greater chance of winning. If Barry chooses $\neg A$ then it does not matter what Carl chooses: he will have probability $1/4$ of winning for either choice. However, Carl's choice will affect Barry's chance of winning. What should Carl do? If he is amiable and can forgive

TABLE 2: Game state outcomes for (1, 1, 1)

		Carl: A	Carl: $\neg A$
Barry	A	(0, 0, 0) (1, 1, 1)	(0, 0, 1) (1, 1, 0)
	$\neg A$	(0, 1, 0) (1, 0, 1)	(0, 1, 1) (1, 0, 0)

TABLE 3: Winning probabilities for (1, 1, 1)

		Carl: A	Carl: $\neg A$
Barry	A	(1/3, 1/3, 1/3)	(1/4, 1/4, 1/2)
	$\neg A$	(1/4, 1/2, 1/4)	(1/2, 1/4, 1/4)

Barry for limiting him to a winning probability of 1/4 then Carl will choose A; if he is vindictive and wants to take Barry down with him then he will choose $\neg A$.

To move forward in our analysis, we make the assumption that Barry and Carl each rank the players in order of preference of winner. Of course each player will rank himself first, leaving only two possibilities for their preferences: he is *Vindictive* if he prefers that Adam win over the other player or *Amiable* if he prefers that the other player win over Adam. In this way we change the original three player game to a two-player *preference game* between Barry and Carl in which the options are Amiable or Vindictive. The payoff matrix for the game is the resulting matrix of winning probabilities and each player is attempting to maximize his winning payoff (probability). TABLE 4 shows the payoff matrix for this game when one point is needed to win (the payoff/probability vectors are transposed).

TABLE 4: Values of $P(1, 1, 1)$ (payoff matrix) for the preference game

		Carl: Amiable	Carl: Vindictive
Barry	Amiable	$\begin{pmatrix} 0.25 \\ 0.5 \\ 0.25 \end{pmatrix}$	$\begin{pmatrix} 0.25 \\ 0.25 \\ 0.5 \end{pmatrix}$
	Vindictive	$\begin{pmatrix} 0.25 \\ 0.5 \\ 0.25 \end{pmatrix}$	$\begin{pmatrix} 0.5 \\ 0.25 \\ 0.25 \end{pmatrix}$

Once we have fixed the preferences of Barry and Carl, we can recursively determine the values of $P(n, n, n)$ for $n \geq 1$. Experimental evidence shows that for $14 \leq n \leq 100$, Barry is better off being vindictive while Carl is better off being amiable. In fact, for these values of n, the strategy of (Vindictive, Amiable) is a *pure Nash equilibrium*—neither player can improve his payoff by unilaterally changing his

strategy [**4**, p. 128]. TABLE 5 shows the possible values of $P(100, 100, 100)$. It is not known if this pattern continues for $n > 100$.

TABLE 5: Values of $P(100, 100, 100)$ for the preference game

		Carl: Amiable	Carl: Vindictive
Barry	Amiable	$\begin{pmatrix} 0.0142 \\ 0.3816 \\ 0.6042 \end{pmatrix}$	$\begin{pmatrix} 0.1210 \\ 0.3229 \\ 0.5561 \end{pmatrix}$
	Vindictive	$\begin{pmatrix} 0.0130 \\ 0.4113 \\ 0.5757 \end{pmatrix}$	$\begin{pmatrix} 0.1266 \\ 0.3337 \\ 0.5397 \end{pmatrix}$

In addition to being Vindictive and Amiable, Barry and Carl may also be *Indifferent*—they have no second choice for winner and will choose randomly between two options that give them the same probability outcome. With this extra option, there are nine possible values of $P(n, n, n)$. TABLE 6 shows the payoff/probability matrix $P(100, 100, 100)$.

TABLE 6: Values of $P(100, 100, 100)$ for the preference game

		Carl: Amiable	Carl: Indifferent	Carl: Vindictive
Barry	Amiable	$\begin{pmatrix} 0.0142 \\ 0.3816 \\ 0.6042 \end{pmatrix}$	$\begin{pmatrix} 0.1043 \\ 0.3497 \\ 0.5460 \end{pmatrix}$	$\begin{pmatrix} 0.1210 \\ 0.3229 \\ 0.5561 \end{pmatrix}$
	Indifferent	$\begin{pmatrix} 0.0108 \\ 0.3971 \\ 0.5920 \end{pmatrix}$	$\begin{pmatrix} 0.1043 \\ 0.3497 \\ 0.5460 \end{pmatrix}$	$\begin{pmatrix} 0.0222 \\ 0.3742 \\ 0.6036 \end{pmatrix}$
	Vindictive	$\begin{pmatrix} 0.0130 \\ 0.4113 \\ 0.5757 \end{pmatrix}$	$\begin{pmatrix} 0.1043 \\ 0.3497 \\ 0.5460 \end{pmatrix}$	$\begin{pmatrix} 0.1266 \\ 0.3337 \\ 0.5397 \end{pmatrix}$

Note that the Amiable choice for Barry is dominated by both the Indifferent and Vindictive choices. Also, the Indifferent choice for Carl is dominated by the Amiable choice. Thus the payoff matrix for the preference game can be pared down to only the Indifferent and Vindictive choices for Barry and the Amiable and Vindictive choices for Carl. In this reduced game there are *two* pure Nash equilibria, one at (Indifferent,Vindictive) and another at (Vindictive, Amiable).

In fact, if we rank the outcomes in order of preference of the players (where 1 is the least preferred and 4 is the most preferred), we obtain TABLE 7, the game of Chicken:

> Two adversaries are set on a collision course. If both persist, then a very unpleasant outcome, sometimes mutual annihilation, is guaranteed. If only one of the players swerves away (chickens) he loses the game. If both swerve, the result is a draw [**4**, p. 125].

TABLE 7: The game of Chicken

		Carl	
		Amiable	Vindictive
Barry	Indifferent	(3, 3)	(2, 4)
	Vindictive	(4, 2)	(1, 1)

In our situation, the "very unpleasant" outcome occurs when both players are Vindictive—they work against each other and give each other the least probabilities to win. While Barry and Carl are still each more likely to win than Adam, they could do even better if they were able (and willing) to cooperate and play the (Indifferent, Amiable) strategy. More information on games like this, where there is no clear strategy for the players, can be found in Stahl [**4**] and Straffin [**6**].

Similar results hold for $5 \leq n \leq 100$ (except $n = 11$, 14, and 17). Further, for all n between 1 and 100, the values of $P(n, n, n)$, given an Indifferent Carl, are all equal. As before, general results are not known for $n > 100$.

Conclusion

In the two-player Singled Out game, the second player has the advantage by playing the contrari-cat strategy. Further, the probability that the second player will win increases to one as the number of points to win increases to infinity. We saw also that the first player can overcome this disadvantage provided that he is able to guess correctly better than $2/3$ of the time.

The more interesting case of three players is still open. Our calculations for small n indicate that, as expected, the third player does have an advantage. But this advantage does not seem to be overwhelming, and it also relies on the third player using the counter-intuitive strategy of working with the second player (who is his closest rival).

Several questions remain. In particular, when Barry and Carl are allowed to be Vindictive or Amiable, will there always be a Nash equilibrium at (Vindictive, Amiable) for large n? Will $P(n, n, n)$ approach a fixed payoff/probability vector? With the Indifferent choice, will the preference game reduce to one of Chicken for large enough n? What effect would communication have on the game? Is there another method of analyzing the three player game other than reducing it to a preference game? And what happens when we play the Singled Out game with N players? What can mathematics tell us about how to win a date?

REFERENCES

1. D. André, Solution directe du problème résolu par M. Bertrand, *Comptes Rendus de l'Académie des Sciences* **105** (1887), 136–7.
2. J. Conway, *Functions of One Complex Variable*, 2nd ed., (*Graduate Texts in Mathematics*, vol. 11), Springer-Verlag, New York, 1978.
3. P. Hilton and J. Pedersen, Catalan numbers, their generalizations, and their uses, *Mathematical Intelligencer* **13** (1991), 64–75.
4. S. Stahl, *A Gentle Introduction to Game Theory*, (*Mathematical World*, vol. 13), American Mathematical Society, Providence, 1999.
5. R. Stanley, *Enumerative Combinatorics*, Cambridge University Press, Cambridge, 1999.
6. P. Straffin, *Game Theory and Strategy*, (*New Mathematical Library*, vol. 36), Mathematical Association of America, Washington, 1993.

Height and Excess of Pythagorean Triples

DARRYL McCULLOUGH
University of Oklahoma
Norman, OK 73019
dmccullough@math.ou.edu

Does the world really need another article about Pythagorean triples? Here is why we think so. The set of Pythagorean triples has a lot of interesting structure, which has intrigued both amateur and professional mathematicians. It is the topic of an extensive mathematical literature, almost all of which relies on an enumeration of primitive Pythagorean triples that has been known since ancient times. But it is not widely known that there is a different enumeration, based on two simple geometric parameters that we call the *height* and the *excess*. In this article, we will use these parameters to make some known results about Pythagorean triples more transparent. And we will use them to achieve a better understanding of one natural group structure on the set of primitive Pythagorean triples, and to discover another one.

Recall that a *Pythagorean triple* (PT) is an ordered triple (a, b, c) of positive integers such that $a^2 + b^2 = c^2$. When a and b are relatively prime, the triple is a *primitive* PT (PPT). Each PT is a positive integer multiple of a uniquely determined PPT.

The height and excess parameters are shown in FIGURE 1. For a PT (a, b, c), the *height* h is just $c - b$, and the *excess* e is $a + b - c$. The term *excess* arises from the fact that e is simply the extra distance one must travel when going along the two legs instead of the hypotenuse.

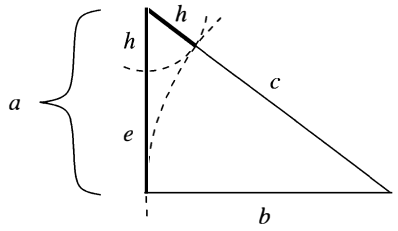


Figure 1 Height and excess of a Pythagorean triangle

Not all combinations of h and e can occur in an integer-sided triangle. We will see that, for a given h, the possible values of e are *exactly the integer multiples of a certain integer d.* The integer d is called the *increment,* and it is related to h in a simple way: d is the smallest positive integer whose square is divisible by $2h$. Since e is a multiple of d, we can write $e = kd$ for a positive integer k. As will be verified in Theorem 1, associating k and h to (a, b, c) sets up a one-to-one correspondence of the PTs with the pairs of positive integers (k, h). For example, everybody's favorite PT (3, 4, 5) corresponds to the pair (1, 1), and (4, 3, 5) and (5, 12, 13) correspond to (1, 2) and (2, 1) respectively, while the nonprimitive PTs (48, 189, 195) and (459, 1260, 1341) correspond to (7, 6) and (21, 81). We call this correspondence the *height-excess enumeration.*

In the rest of this article, we will see various uses of the height and excess parameters. The overarching goal is *to find structure on the set of Pythagorean triples.* To best understand a particular structure on the set of PTs, we need to *view it with the*

right coordinates. The classical enumeration, which we will detail later, assigns a pair of relatively prime integer coordinates (m, n) to each PPT. The height and excess parameters lead to several other systems of coordinates, and we will use whichever of these systems of coordinates seems best for viewing the structure that we are trying to understand. Besides the *k-h* coordinates coming from the height-excess enumeration, and a closely-related kind of coordinates on PPTs, called *k-q* coordinates, we will use *a-h* coordinates, in which (3, 4, 5) is [3, 1], and *e-h* coordinates, in which (3, 4, 5) is $\langle 2, 1\rangle$. Each of these coordinate systems reveals some of the structure of the set of PTs that is hidden when the PTs are written in the conventional way. In fact, it sometimes seems to me that (a, b, c) is the most unenlightening way to think about a PT.

The height-excess enumeration

Our first theorem will establish the height-excess enumeration of PTs. It actually enumerates *all* the triples of (not necessarily positive) integers satisfying the Pythagorean relation $a^2 + b^2 = c^2$. These are called *generalized Pythagorean triples* (GPTs). A GPT (a, b, c) is called primitive when a and b are relatively prime. Each GPT is a positive integer multiple of a uniquely determined primitive GPT.

The PTs (a, b, c) and (b, a, c) both correspond to the same geometric right triangle. We make the arbitrary choice of thinking of the one with $a < b$ as representing this right triangle, so we use the term *Pythagorean triangle* to mean a PT with $a < b$. Theorem 1 will identify, in terms of k and h, the PTs that are triangles, and the PTs that are primitive.

In the statement of Theorem 1, the symbol e does not appear explicitly. The excess is the number dk. Also, a nonzero integer is called *square-free* if it is not divisible by the square of any prime.

THEOREM 1. (THE HEIGHT-EXCESS ENUMERATION) *For any (k, h) in the set $\mathbb{Z} \times \mathbb{Z}$ of pairs of integers, define $P(k, h)$ as follows: If h is nonzero, write it as pq^2 with p square-free and q positive, and associate with it the number d equal to $2pq$ if p is odd, and to pq if p is even. Put*

$$P(k, h) = \left(h + dk, dk + \frac{(dk)^2}{2h}, h + dk + \frac{(dk)^2}{2h}\right),$$

if $h \neq 0$, and put $P(k, 0) = (0, k, k)$. Then P is a bijection from $\mathbb{Z} \times \mathbb{Z}$ to the set of all GPTs (a, b, c). Moreover,

1. *$P(k, h)$ is primitive if and only if k and h are relatively prime and either $h = \pm q^2$ with q odd, or $h = \pm 2q^2$.*
2. *$P(k, h)$ is a PT if and only if both k and h are positive, and is a Pythagorean triangle when in addition $k > \sqrt{2}h/d$.*

Theorem 1 gives a recipe for finding the parameters k and h for any GPT (a, b, c). If $b = c$, then the triple is $(0, k, k) = P(k, 0)$. Otherwise, k and h are calculated as follows.

To find (k, h) from (a, b, c)

1. Put $h = c - b$.
2. Write $h = pq^2$ with p square-free and positive.
3. Put $d = 2pq$ if p is odd, and $d = pq$ if p is even.
4. Put $k = (a - h)/d$.

For example, for $(459, 1260, 1341)$, we have $h = 1341 - 1260 = 81$, so $p = 1$ and $q = 9$, giving $d = 18$, and $k = (459 - 81)/18 = 21$, so $(459, 1260, 1341)$ is $P(21, 81)$.

The proof of Theorem 1 uses only the basic properties of prime factorization and relatively prime integers, and some college algebra. It could be skipped on a first reading, in order to get on to some of the flashier applications of height and excess.

The first step of the proof is to develop the key properties of d. As usual, the notation $x \mid y$ means that the integer y is evenly divisible by the integer x.

LEMMA 1. *Let h be a nonzero integer with associated increment d, as defined in Theorem 1. Then $2h \mid d^2$. If D is any integer for which $2h \mid D^2$, then $d \mid D$.*

Proof. The first assertion is immediate from the definition of d. For the second, we may assume that D is nonzero. Considering prime factorizations, we see that if $2h = 2pq^2$ divides D^2, then $q \mid D$, so $D = D_1 q$ and $2p \mid D_1^2$. Since p has distinct prime factors, it follows that $p \mid D_1$, and if p is odd then $2p \mid D_1$, so $d \mid D$. ∎

Now for the actual proof of Theorem 1. For $h = 0$, all its assertions are straighforward to check, so we assume that $h \neq 0$. By Lemma 1, every expression $P(k, h)$ has integer entries, and algebra shows that it is Pythagorean. Using $h = c - b$, $e = a + b - c$, and the Pythagorean relation, more algebra shows that for all GPTs,

$$(a, b, c) = \left(h + e, e + \frac{e^2}{2h}, h + e + \frac{e^2}{2h}\right).$$

The Pythagorean relation implies that $e^2 = 2(c - a)(c - b)$, so $2h \mid e^2$. By Lemma 1, e is divisible by d, say $e = dk$. So every GPT has the form $P(k, h)$. Since the GPT determines h, e, and d uniquely, k is also determined, showing that P is injective.

Next we identify the primitive GPTs. We use the notation $\gcd(x, y)$ to denote the greatest common divisor of two integers x and y, not both 0. For $h = 0$, $P(k, 0) = (0, k, k)$ is primitive exactly when $k = \pm 1$, and $(\pm 1, 0)$ are exactly the pairs with $h = 0$ that satisfy the given conditions. Suppose that $h \neq 0$. When (a, b, c) is a primitive PT, $c - a$ and $c - b$ must be relatively prime. For suppose that both were divisible by some prime r. Then r divides the sum $(c - a)^2 + (c - b)^2 = (3c - 2a - 2b)c$. Now r could not divide c, since then it would divide both a and b. So r divides $3c - 2a - 2b = 2(c - a) + 2(c - b) - c$. Again we have the contradiction that r divides c. We conclude that $c - a = (k^2 d^2)/(2h)$ and $c - b = h$ are relatively prime. For p odd, these are $2pk^2$ and pq^2, so $p = \pm 1$, q is odd, and $\gcd(2k, q) = 1$. For p even, they are $k^2 p/2$ and pq^2, so $p = \pm 2$ and $\gcd(k, 2q) = 1$. Thus $\gcd(k, h) = 1$ in both cases. Conversely, suppose that h and k satisfy the given conditions. For $h = \pm q^2$, (a, b) is $\pm(q(q + 2k), 2k(q + k))$. If r is a prime dividing both entries, then $r \neq 2$ since the first entry is odd. So r must divide q or $q + 2k$, and must divide k or $q + k$. Any of the four possible combinations leads to r dividing both q and k, a contradiction. For $h = \pm 2q^2$, (a, b) is $\pm(2q(k + q), k(q + 2k))$ and the reasoning is similar.

For the additional remarks, suppose first that $P(k, h) = (a, b, c)$ is a PT, that is, that all three of a, b, and c are positive. Since $P(k, 0) = (0, k, k)$, we must have $h \neq 0$. Since $c = (h^2 + (e + h)^2)/(2h)$, c is positive exactly when $h > 0$. For $h > 0$, $b = dk + (dk)^2/(2h)$ is positive exactly when $(h + dk)^2 > h^2$, that is, either $h + dk < -h$ or $h + dk > h$. In the first case, $a < 0$ and in the second case $a > 0$. We conclude that $P(k, h)$ is a PT exactly when both h and k are positive. For PTs, the form given in Theorem 1 is a triangle exactly when $h + dk < dk + (dk)^2/(2h)$, which says that $k > \sqrt{2}h/d$. ∎

We will now list some properties of the height-excess enumeration. Except for the description of the excess as twice the inradius, they are not used in this article, but some might be of interest in other contexts. We will finish this section with some history of the enumeration.

The number k equals $4A/(dP)$, where A is the area $ab/2$ and P is the perimeter $a+b+c$. This can be seen using the identity $eP = 4A$, which follows from the Pythagorean property. For a right triangle, e is twice the inradius, that is, twice the radius of the largest circle that can be inscribed in the triangle. To see this, just draw the radii from the center of this circle to the three points where it meets the sides and use the definition of excess.

When $h > 0$ and $k > 0$, k is the ordinal of (a, b, c) in the sequence of PTs of height h, in order of increasing values of any one of: a, b, b/a, A, P. This illustrates what I like most about the height-excess enumeration: unlike the classical enumeration (which we will discuss later), it brings order to the apparent chaos of nonprimitive triples, and puts them on an equal footing with the overprivileged primitive triples.

For $h > 0$, d satisfies $2\sqrt{h} \le d \le 2h$, with the lower bound achieved when $p = 1$ and the upper bound when $q = 1$. Thus, the size of d relative to $2\sqrt{h}$ is a rough measure of how far h is from being a perfect square. In fact, the expression $d^2/(2h)$ that appears in Theorem 1 is exactly $p/2$, when p is even, or $2p$, when p is odd.

As far as we can determine, the first version of the height-excess enumeration for PTs is due to M. G. Teigan and D. W. Hadwin [**23**]. The parameters used there are $x = h$, $y = e^2/(2h)$ (which, being $c - a$, is the height of (b, a, c)), and $z = e$. It was noted that (1) z is even, and (2) $2xy = z^2$, and conversely that any triple of positive integers (x, y, z) satisfying (1) and (2) determines a PT, which is primitive exactly when $\gcd(x, y) = 1$. The height-excess enumeration was also found by H. Klostergaard [**16**]. The integer n in [**16**] is our $e/2$, and the integer called d there is our h. Klostergaard observed that h divides $e^2/2$, and used this to describe an enumeration of all Pythagorean triangles by finding the possible heights associated to each increasing integer value of $e/2$; also, $e/2$ is described as twice the area-perimeter ratio.

More explicit renderings of the height-excess enumeration were given by B. Dawson [**7**] and M. Wójtowicz [**26**]. For positive h, Dawson's parameterization is (r, h) where $r = a/d$ if h is even and $r = a/d - 1/2$ if h is odd [**7**]. This shifts the first coordinate so that $(0, h)$ corresponds to the GPT of height h with the smallest nonnegative value of a. Wójtowicz [**26**, Theorem 6] gave a formula equivalent to the one in Theorem 1. Also, A. Grytczuk [**9**] obtained a ring structure (without unit) on the set $\mathcal{P}_h$ of GPTs of height h by transferring the usual structure on the subring $d\mathbb{Z}$ of $\mathbb{Z}$ to $\mathcal{P}_h$ via the bijection sending $P(k, h)$ to e, and this was elaborated upon by Wójtowicz [**25**].

The height-excess enumeration for PTs is implicit as well in an article written by the father-and-son combination of P. W. Wade and W. R. Wade [**24**]. They found the number d, developed a recursion formula that produces all PTs of height h, and used the classical enumeration to give a full verification that the recursion produces all PTs in the cases $h = q^2$ and $h = 2q^2$. In an article that I wrote with Elizabeth Wade [**18**], we proved Theorem 1 for the case of PTs, and used it to give a quick verification of the Wade-Wade recursion for all positive h. In fact, the recursion gives $P(k+1, h)$ in terms of $P(k, h)$.

Elizabeth is not related to P. W. and W. R.

PTs of a given excess The problem of finding all PPTs and PTs (a, b, c) with a equal to a given number has been solved several times in the literature [**1, 4, 14**]. In fact, there is currently a website where one can enter a value of a and receive a list of the PTs [**5**]. As an application of Theorem 1, we are going to obtain a similar count of the number of PTs with a given excess. Our result gives the exact counts both of PTs

and PPTs, and, as we will explain, its proof provides an effective procedure for listing them. We remark that e is always even, since (among many possible reasons) $e = dk$ and d is always even.

THEOREM 2. *For an even positive integer E, write E as $2^{\alpha_0} p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ for distinct odd primes p_i, with all $\alpha_i > 0$. Then the number of PTs of excess E is*

$$2\alpha_0 \prod_{i=1}^{n} (2\alpha_i + 1),$$

of which exactly 2^{n+1} are primitive.

The PTs in Theorem 2 occur in pairs (a, b, c) and (b, a, c), so to obtain the number of Pythagorean triangles of excess E we divide the number of PTs by 2.

Proof. We first find the PPTs $P(k, h)$ with excess E. By statement 1 of Theorem 1, there are two cases. If $h = q^2$, then $d = 2q$, q is odd, and $\gcd(k, q) = 1$. Thus we need to factor $E = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ as $2qk$. Since q and k can have no prime factors in common, when q has some powers of a prime it must have them all. Thus, the choices for q are the 2^n products of the form $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_r}^{\alpha_{i_r}}$, where $i_1 < \cdots < i_r$. This yields the PPTs $P(E/2q, q^2)$ with $d = 2q$ and excess E. Similarly, if $h = 2q^2$, then again $d = 2q$, but $\gcd(k, 2q) = 1$, so k must be odd. In this case there are 2^n choices for k and so 2^n PPTs of the form $P(E/2q, 2q^2)$. Thus we have a total of 2^{n+1} choices for PPTs of excess E.

To include nonprimitive triples, we need to count 2^{r+1} triples for each divisor of E of the form $D = 2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$ (with all exponents positive). These are the PPTs of excess D, and multiplied by E/D they give triples of excess E. Each term in the product $2\alpha_0 \prod_{i=1}^{n} (2\alpha_i + 1)$ has the form $2^{r+1}\alpha_0\alpha_{i_1} \cdots \alpha_{i_r}$. To obtain a divisor D of the form $2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$, one has α_0 choices for β_0 and α_{i_j} choices for each β_{i_j}, giving $\alpha_0\alpha_{i_1} \cdots \alpha_{i_r}$ possibilities. Each such choice produces 2^{r+1} triples, so the number of triples arising from the divisors of the form $D = 2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$ is exactly $2^{r+1}\alpha_0\alpha_{i_1} \cdots \alpha_{i_r}$. ∎

The proof of Theorem 2 gives a procedure to find the PTs or Pythagorean triangles of excess E. Take each even divisor D of E, written as $D = 2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$. For each of the 2^r choices of $\{j_1, \ldots, j_k\} \subset \{i_1, \ldots, i_r\}$, write $D = xy$ with $y = p_{j_1}^{\beta_{j_1}} \cdots p_{j_k}^{\beta_{j_k}}$. Each such factorization gives two PTs $\frac{E}{D} P(x/2, y^2)$ and $\frac{E}{D} P(y, x^2/2)$ of excess E. They have the same values of a and b, but in reverse order. The one with smaller a gives the Pythagorean triangle.

For example, for $E = 36 = 2^2 \cdot 3^2$ there are ten triangles, including two primitives. The procedure finds them to be

$$\begin{array}{llll} (37, 684, 685), & (38, 360, 362), & (39, 252, 255), & (40, 198, 202), \\ (42, 144, 150), & (44, 117, 125), & (45, 108, 117), & (48, 90, 102), \\ & (54, 72, 90), & \text{and} & (60, 63, 87). \end{array}$$

FIGURE 2 shows these ten triangles, with the two primitive ones, (37, 684, 685) and (44, 117, 125), emphasized. The hypotenuses of these ten triangles do not actually intersect in a single point, as the figure may seem to suggest. In fact, for no three triangles of the same excess (Pythagorean or not, positioned as in FIGURE 2 in the first quadrant with their right angles at the origin) do the hypotenuses intersect in a common point; for as we noted in the previous section, the excess equals the diameter of the

incircle, so the hypotenuses of the three triangles T_1, T_2, T_3 would be tangent to their common incircle at distinct points p_1, p_2, and p_3. Selecting notation so that p_1, p_2, and p_3 have increasing x-coordinate, we see that the intersections of the hypotenuses of T_1 and T_2 and of T_2 and T_3 lie on opposite sides of p_2 in the hypotenuse of T_2. So there is no common point.

Figure 2 The ten Pythagorean triangles of excess 36

If we do not restrict to triangles with the same excess, then arbitrarily large numbers of Pythagorean triangles, positioned as in FIGURE 2, may have hypotenuses sharing a common point. For if p/q is a rational number greater than 1, the triangle with vertices $(p/q, 0)$, $(0, 0)$, and $(0, p/(p-q))$ will have hypotenuse passing through $(1, 1)$. The length of its hypotenuse is the square root of $p^2((p-q)^2+q^2)/(q^2(p-q)^2)$, which will be rational provided that $p-q$ and q form the first two entries of a PT. Selecting n such numbers $p_1/q_1, \ldots, p_n/q_n$, then multiplying by the number $Q = q_1 \cdots q_n(p_1 - q_1) \cdots (p_n - q_n)$ to clear the denominators of the fractions, we obtain n Pythagorean triangles whose hypotenuses pass through the point (Q, Q). Can this happen with primitive Pythagorean triangles?

The classical enumeration of primitive PTs We mentioned that most articles on PTs rely on the *classical enumeration*, which dates to antiquity [**4, 6**]. It appears in almost every text on elementary number theory, and goes like this. For any pair (m, n) of positive integers with $m > n$, the triples $(m^2 - n^2, 2mn, m^2 + n^2)$ and $(2mn, m^2 - n^2, m^2 + n^2)$ are Pythagorean and correspond to a single Pythagorean triangle. If m and n are relatively prime and not both odd, then these PTs are primitive. Conversely, an argument using prime factorization shows that every PPT has one of these two forms, with m and n relatively prime and not both odd. So, taking these triples for all relatively prime pairs (m, n) with $m > n$ and not both odd produces each PPT exactly once, while taking all their integer multiples gives each PT once. As explained in [**4**], there is a slightly nicer *refined classical enumeration.* Start instead with all relatively prime (m, n) with $m > n$, and write $(m^2 - n^2, 2mn, m^2 + n^2)$ if one of m or n is even (that is, when a is odd), and

$$\left(\frac{m^2 - n^2}{2}, mn, \frac{m^2 + n^2}{2}\right)$$

if m and n are both odd (when a is even). This gives a list of PPTs, with each one appearing exactly once.

For PPTs, the height-excess enumeration gives the following enumeration.

COROLLARY 1. *Let (a, b, c) be a PPT.*

1. *If a is odd, then (a, b, c) can be expressed uniquely as $P(k, q^2) = (q^2 + 2qk, 2qk + 2k^2, q^2 + 2qk + 2k^2)$ for some (k, q) with $\gcd(2k, q) = 1$.*
2. *If a is even, then (a, b, c) can be expressed uniquely as $P(k, 2q^2) = (2q^2 + 2qk, 2qk + k^2, 2q^2 + 2qk + k^2)$ for some (k, q) with $\gcd(k, 2q) = 1$.*

Proof. From Theorem 1, the $P(k, q^2)$ with $\gcd(2k, q) = 1$ are exactly the PPTs with a odd, while the $P(k, 2q^2)$ with $\gcd(k, 2q) = 1$ are exactly those with a even. ∎

How are the refined classical m-n coordinates related to the k-q coordinates coming from Corollary 1? Starting from (m, n), we can use the recipe for finding (k, h) from (a, b, c) to find that $(k, h) = (n, (m-n)^2)$ when one of m or n is even, and $(k, h) = (n, (m-n)^2/2)$ when both are odd. So, $k = n$ in either case, and (using the fact that $m > n$) we have $q = m - n$ when one of m or n is even, and $q = (m-n)/2$ when both are odd. Suppose, on the other hand, that we start from (k, q). Then $q = m - n$ and $(m, n) = (k + q, k)$ when a is odd, while $q = (m-n)/2$ and $(m, n) = (k + 2q, k)$ when a is even.

Corollary 1 is similar to the reparameterization of the classical enumeration obtained in [**6**] by putting $m = i + j$ and $n = i$.

The Barning tree

A very different approach to enumerating the PPTs appears in works of a number of authors [**3, 10, 11, 13, 15, 17, 21**]. We believe that the original version is due to F. J. M. Barning [**3**]. He considered the set of PPTs with a even, regarding them as column vectors. In (a, b, c) coordinates, the statement is quite striking:

THEOREM 3. *Consider the following transformations, each having determinant* 1:

$$A_1 = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}.$$

Every PPT (a, b, c) *with* a *even can be obtained in exactly one way starting from* $(4, 3, 5)$ *and applying a sequence of the transformations* A_i.

In terms of *structure* on the set of PPTs, this can be interpreted as saying that the PPTs with even a form the vertices of a directed tree with three edges leaving each vertex, and one entering every vertex except $(4, 3, 5)$, in such a way that multiplication of a PPT by an A_i sends it to one of the three vertices to which it leads in the tree. Because of this interpretation, we call this enumeration the *Barning tree*. The PPTs with odd a have a corresponding structure, as we will see near the end of this section.

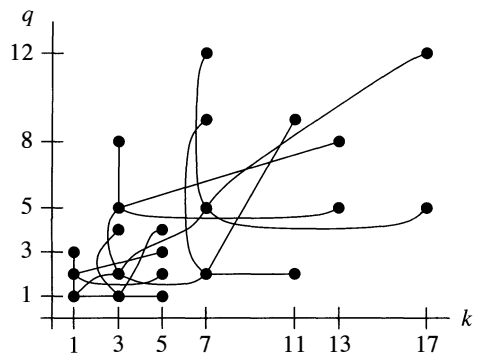


Figure 3 A portion of the Barning tree, viewed in k-q coordinates

Our proof of Barning's theorem uses the k-q coordinates on PPTs given in part 2 of Corollary 1 (we have not been able to obtain a copy of Barning's article, but our proof is surely just a recasting of the original).

FIGURE 3 shows a portion of the Barning tree in k-q coordinates. The vertices are some of the (k, q) pairs that correspond to PPTs, and the edges connect each vertex to the three PPTs obtained from it by multiplying by one of the three matrices. Notice that each vertex and its three offspring form a rectangle. The proof uses a clever process for starting at any vertex and descending through the tree down to the vertex $(1, 1)$, which is the PT $(4, 3, 5)$ in k-q coordinates. We call this process the *Barning descent.*

Proof of Theorem 3. For positive k and q with $\gcd(k, 2q) = 1$, write $T(k, q)$ to denote the PPT $P(k, 2q^2) = (2q^2 + 2qk, 2qk + k^2, 2q^2 + 2qk + k^2)$ (when necessary in calculations, assume that $T(k, q)$ is a column vector rather than a row vector). In particular, $T(1, 1) = (4, 3, 5)$. Corollary 1 shows that these are exactly the PPTs with a even. We calculate

$$A_2\, T(k, q) = \begin{pmatrix} 6q^2 + 10qk + 4k^2 \\ 8q^2 + 10qk + 3k^2 \\ 10q^2 + 14qk + 5k^2 \end{pmatrix}.$$

Calling this vector (A, B, C), we use our usual recipe to write it as $T(K, Q)$ by computing that $H = C - B = 2(q + k)^2$, so $Q = q + k$, $D = 2(q + k)$, and $K = (A - H)/D = (4q^2 + 6qk + 2k^2)/2(q + k) = k + 2q$. Carrying out similar calculations for A_1 and A_3, we find:

$$\begin{aligned} A_1\, T(k, q) &= T(k, q + k), \\ A_2\, T(k, q) &= T(k + 2q, k + q), \\ A_3\, T(k, q) &= T(k + 2q, q). \end{aligned}$$

Notice that when we write $A_i\, T(k, q)$ as $T(K, Q)$, we have $K < Q$ in the first case, $Q < K < 2Q$ in the second, and $2Q < K$ in the third.

In k-q coordinates, the matrices of A_1, A_2, and A_3 are

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Inverting these matrices, and, as before, denoting $A_i\, T(k, q)$ by $T(K, Q)$, we find that:

$$\begin{aligned} A_1^{-1} T(K, Q) &= T(K, Q - K), \\ A_2^{-1} T(K, Q) &= T(2Q - K, K - Q), \\ A_3^{-1} T(K, Q) &= T(K - 2Q, Q). \end{aligned}$$

These three cases are illustrated in FIGURE 4, where P_i denotes $A_i^{-1}\, T(K, Q)$.

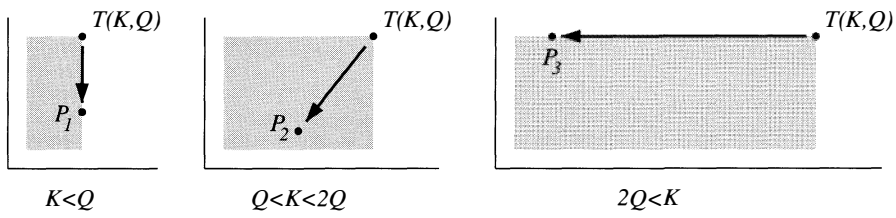


Figure 4 The three cases in the Barning descent

We are now set up for the Barning descent. Given any $T(K, Q)$ with $K > 1$ or $Q > 1$, the condition that $\gcd(K, 2Q) = 1$ shows that either $K < Q$, $Q < K < 2Q$, or $2Q < K$. Applying A_1^{-1}, A_2^{-1}, or A_3^{-1} in the respective cases produces a $T(k, q)$ with $k + q < K + Q$. Repeating with this new PPT, we find a composition $A_{i_n}^{-1} \cdots A_{i_1}^{-1}$ sending $T(K, Q)$ to $T(1, 1)$. The composition $A_{i_1} \cdots A_{i_n}$ moves $T(1, 1)$ to $T(K, Q)$. This is the only possible such composition, for any other one would lead to a case where $A_i\, T(k', q') = A_j\, T(k'', q'')$ with $i \neq j$, but this resulting element $T(K', Q')$ would have to satisfy two of the mutually exclusive conditions $K' < Q'$, $Q' < K' < 2Q'$, and $2Q' < K'$. ■

The Barning tree for the PPTs with a odd is essentially the same as the version for a even, but we need not repeat the entire argument. Notice that for the matrix

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

one has (as usual thinking of (a, b, c) as a column vector) that $M(a, b, c) = (b, a, c)$. Since in a PPT, exactly one of a or b is even, multiplication by M converts the PPTs with a odd into the PPTs with a even, and converts the even ones back into odds. So, the exact statement of Theorem 3 holds after replacing each A_i by MA_iM and replacing (4, 3, 5) by (3, 4, 5).

Two articles by L. Palmer, M. Ahuja, and M. Tikoo **[19, 20]** contain some additional information about the form of a matrix A that preserves the set of PTs.

Operations on PTs

In the remainder of this article, we will be examining algebraic operations on sets of GPTs. There are many meaningless operations—for example, we could just make a list of all the GPTs in some random order, associate the nth GPT to the natural number n, and "add" the PTs according to the way that their associated numbers add. An operation is meaningful only when it reflects geometric or algebraic information about the GPTs.

When developing algebraic structures, one often uses a procedure called *projectivization.* This is actually a familiar process from everyday arithmetic. Start with the set of ordered pairs of positive integers (m, n). Let us write this pair as $m/\!/n$, and consider the simple operation defined by $m_1/\!/n_1 * m_2/\!/n_2 = m_1m_2/\!/n_1n_2$. This makes the set into a *semigroup,* that is, a set with an associative operation. In this case, the operation has an identity element, since $1/\!/1 * m/\!/n = m/\!/n$, so the semigroup is called a *monoid.* But it fails to be a *group,* since some elements (in fact, all elements other than $1/\!/1$) do not have inverses. Now, we projectivize by declaring that $m/\!/n$ and $r/\!/s$ are equivalent if they have integer multiples that are equal (that is, if there are positive integers t and u so that $tm/\!/tn = ur/\!/us$). We write m/n for the set of pairs equivalent to $m/\!/n$. For example, $3/6 = \{1/\!/2, 2/\!/4, 3/\!/6, 4/\!/8, \ldots\} = 1/2$. The equivalence relation has the property that if $m_1/n_1 = m_2/n_2$ and $r_1/s_1 = r_2/s_2$, then $m_1r_1/n_1s_1 = m_2r_2/n_2s_2$, so the star operation induces a multiplication operation on the equivalence classes defined by $m/n * r/s = mr/ns$. This operation still has an identity element, $1/1$, but now every element has an inverse, since $a/b * b/a = ab/ba = 1/1$. The equivalence classes form the group $\mathbb{Q}_{>0}$ of positive rational numbers. One can think of this process as erasing a lot of inessential structure on the fractions—the structure that makes $2/\!/4$ different from $3/\!/6$—and after eliminating this unnecessary structure, the higher-level algebraic structure of a group can exist on the set $\mathbb{Q}_{>0}$ of equivalence classes.

For the rational numbers, each equivalence class m/n contains exactly one fraction in lowest terms, and two fractions are equivalent exactly when they are both multiples of the same fraction in lowest terms. In everyday life, we often identify a rational number with the unique fraction in lowest terms that it contains, as when we write $(2/3)(9/4) = 3/2$. What we are really doing is multiplying the fractions $2/\!/3$ and $9/\!/4$ to obtain $18/\!/12$, then writing the equivalence class $18/12$ as $3/2$.

Another way to think of this equivalence relation is that the underlying meaning of a fraction is a *ratio,* and $1/\!/2$ and $2/\!/4$ just represent the same ratio by different sizes of numbers. In the same way, we can think of the PTs (3, 4, 5) and (6, 8, 10) as the same *shape* (similarity class) of right triangles, just being represented by different sizes of triangles. The PPT (3, 4, 5) is the triple in "lowest terms" that represents this shape (just as $1/2$ is the "primitive" fraction that represents its ratio).

Using the analogous projectivization process on PTs, complex multiplication has been used to construct a well-known operation on the set of PPTs (together with (1, 0, 1)) [**8, 22**]. We call it the Taussky-Eckert operation. One treats the first two entries of (a, b, c) as $a + bi$ and mimics complex multiplication. If the product lies in the second quadrant, multiply by $-i$ to move it into the first quadrant. In formulas, $(a_1, b_1, c_1) \otimes (a_2, b_2, c_2)$ equals $(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1, c_1c_2)$ if $a_1a_2 - b_1b_2 > 0$, and equals $(a_1b_2 + a_2b_1, b_1b_2 - a_1a_2, c_1c_2)$ if $a_1a_2 - b_1b_2 \leq 0$. This defines an operation on the set of PTs, plus the GPTs of the form $(n, 0, n)$ with $n > 0$. The operation is meaningful because it is *multiplicative with respect to the c-coordinate.*

The $\otimes$ operation has an identity element (1, 0, 1), but elements other than (1, 0, 1) do not have inverses, and a product of two PPTs need not be primitive. Again we save the day by declaring that two of these GPTs are equivalent when they have integer multiples that are equal. The operation respects the equivalence relation, so there is an induced operation on the equivalence classes. Also, each equivalence class contains exactly one primitive triple, so the equivalence classes can be identified with the PPTs (along with (1, 0, 1)). At the level of PPTs, this means carrying out the operation, then dividing out by the greatest common divisor to obtain a new PPT. For the equivalence classes, (b, a, c) is the inverse of (a, b, c), because $(a, b, c) \otimes (b, a, c) = (a^2 + b^2, 0, c^2)$, which is equivalent to (1, 0, 1). So just as with fractions and rational numbers, the equivalence classes have the higher-level algebraic structure of a group. Eckert [**8**] showed that with this operation, the PTs form a free abelian group generated by the triples (a, b, p) with $a > b$ and p a prime of the form $4n + 1$ (Hlawka [**12**] gives a discussion of this and other more advanced topics on PTs).

The Beauregard-Suryanarayan group

R. Beauregard and E. Suryanarayan [**4**] studied the operation on the set of GPTs defined by $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2)$. This operation is meaningful because it is multiplicative for a. By projectivizing, they obtained a group structure on the set of primitive GPTs with $a > 0$ and $c > 0$, and identified the resulting group with the group $\mathbb{Q}_{>0}$ of positive rational numbers.

We are going to analyze the Beauregard-Suryanarayan operation using a-h coordinates. That is, we write a GPT (with $h \neq 0$) as $[a, h]$, where a is the a from (a, b, c) and h is the height. We will see that, in these coordinates, the operation behaves as coordinatewise multiplication $[a_1, h_1] * [a_2, h_2] = [a_1a_2, h_1h_2]$. This allows a simplified treatment of the theory developed in [**4**]. The projectivized object obtained from the set of all GPTs with $h \neq 0$ is naturally identified with the monoid $\{1, -1\} \times \mathbb{Q}$, the Beauregard-Suryanarayan group being the subset identified with $\{1\} \times \mathbb{Q}_{>0}$. The PPTs correspond to the semigroup $\{1\} \times \mathbb{Q}_{>1}$.

To get started, observe that the Pythagorean identity implies that for any GPT with $h \neq 0$,

$$(a, b, c) = \left(a, \frac{a^2 - h^2}{2h}, \frac{a^2 + h^2}{2h}\right).$$

Thus, a and h determine a GPT, provided of course that a has the form $a = h + kd$. We denote this GPT by $[a, h]$, and call these the *a-h coordinates* of the GPT. It is a PT exactly when $a > h > 0$, since this is exactly when both h and k are positive. Some interesting examples of GPTs in *a-h* coordinates are:

1. $[1, 1] = (1, 0, 1)$, $[1, -1] = (1, 0, -1)$, $[-1, 1] = (-1, 0, 1)$, and $[-1, -1] = (-1, 0, -1)$.
2. $[3, 1] = (3, 4, 5)$ and $[4, 2] = (4, 3, 5)$, while $[2, 1]$ does not represent a GPT since for $h = 1$ we have $d = 2$.
3. For q odd, $[q, 1] = (q, (q^2 - 1)/2, (q^2 + 1)/2)$.
4. For q odd, $[q, q^2] = (q, (1 - q^2)/2, (q^2 + 1)/2)$.
5. For $s > 1$, $[2^s, 2] = (2^s, 2^{2s-2} - 1, 2^{2s-2} + 1)$.
6. For $s > 1$, $[2^s, 2^{2s-1}] = (2^s, 1 - 2^{2s-2}, 2^{2s-2} + 1)$.

The result of the Beauregard-Suryanarayn operation,

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2),$$

has height

$$b_1b_2 + c_1c_2 - (b_1c_2 + b_2c_1) = (c_1 - b_1)(c_2 - b_2),$$

so written in *a-h* coordinates, the operation takes the form

$$[a_1, h_1] * [a_2, h_2] = [a_1a_2, h_1h_2],$$

as claimed.

Let $\mathcal{D}$ denote the set of GPTs with $h \neq 0$. If $[a, h] = (a, b, c)$ is a GPT and n is a nonzero integer, then $n[a, h] = (na, nb, nc) = [na, nh]$. So just as for the Taussky-Eckert operation, we can projectivize $\mathcal{D}$ by declaring that two GPTs are equivalent if they have positive integer multiples that are equal. For example, the equivalence class of $(4, 3, 5)$ is $\{[4, 2], [8, 4], [12, 6], \ldots\}$. Each equivalence class contains one primitive GPT, so the resulting set of equivalence classes $\mathcal{G}$ can be identified with the set of primitive GPTs of nonzero height. The main result is:

THEOREM 4. *Define $\phi: \mathcal{G} \to \{1, -1\} \times \mathbb{Q}$ by sending $[a, h]$ to $(\sigma(h), a/h)$, where $\sigma(h) = 1$ if h is positive and is -1 if h is negative. Then ϕ is an isomorphism.*

Proof. If $n_1[a_1, h_1] = n_2[a_2, h_2]$, then $\phi([a_1, h_1]) = (\sigma(n_1h_1), n_1a_1/(n_1h_1)) = (\sigma(n_2h_2), n_2a_2/(n_2h_2)) = \phi([a_2, h_2])$, so ϕ is well-defined on equivalence classes. The homomorphism condition $\phi([a_1, h_1] * [a_2, h_2]) = \phi([a_1a_2, h_1h_2])$ is also immediate. For surjectivity, it is enough to note that $\phi(\pm[1, 1]) = (\pm 1, 1)$, $\phi(\pm[1, -1]) = (\pm 1, -1)$, $\phi([0, 1]) = (1, 0)$, $\phi([4, 2]) = (1, 2)$, $\phi([2, 4]) = (1, 1/2)$, and for q an odd prime, $\phi([q, 1]) = (1, q)$ and $\phi([q, q^2]) = (1, 1/q)$, since products of these elements produce all elements of $\{1, -1\} \times \mathbb{Q}$. For injectivity, suppose that $\phi([a_1, h_1]) = \phi([a_2, h_2])$. Then h_1 and h_2 have the same sign, so replacing both $[a_i, h_i]$ by $[-a_i, -h_i]$, if necessary, we may assume that both h_1 and h_2 are positive. Since

$$\frac{1}{h}[a, h] = \left(\frac{a}{h}, \frac{(a/h)^2 - 1}{2}, \frac{(a/h)^2 + 1}{2}\right),$$

we have $h_2[a_1, h_1] = h_1[a_2, h_2]$. That is, $[a_1, h_1]$ and $[a_2, h_2]$ are projectively equivalent, so they represent the same element of $\mathcal{G}$. ∎

Since $\mathbb{Q}_{>0}$ is the free abelian group on the set of primes, this shows that the projectivization of the submonoid consisting of all $[a, h]$ with $a > 0$ and $h > 0$ (that is, the (a, b, c) with $a > 0$ and $c > 0$) is an abelian group that is free on the set $\{[4, 2]\} \cup \{[p, 1] \mid p \text{ is an odd prime}\}$. This is the Beauregard-Suryanarayan group. It has an elegant geometric interpretation, which is explained in [**4**]. Finally, from the formula for (a, b, c) in terms of a and h, we observe that $[a, h]$ is a PT exactly when $a > 0$, $h > 0$, and $a > h$, so the PPTs correspond to the semigroup $\{1\} \times \mathbb{Q}_{>1}$.

The Beauregard-Suryanarayan monoid

To obtain the Beauregard-Suryanarayan group, we projectivized the Beauregard-Suryanarayan monoid, thereby erasing the structure that was preventing it from being a group. In fact, that lost structure is rather interesting, so we will now backtrack and analyze the Beauregard-Suryanarayan monoid itself. This is a good example of how a complicated algebraic object can be understood by studying it "at each prime."

Recall that the Beauregard-Suryanarayan monoid $\mathcal{D}$ was the set of all GPTs $[a, h]$ with $h \neq 0$, with the operation $[a_1, h_1] * [a_2, h_2] = [a_1a_2, h_1h_2]$. We emphasize that the operation is commutative, and remind the reader that a semigroup is a set with an associative operation, while a monoid is a semigroup with an identity element.

The structure we will find involves a direct sum of monoids. The books that I have checked either do not define a direct sum of monoids, or define it in a very abstract setting using the language of categories. Here is a straightforward definition for the countable commutative monoids that we will be using. Suppose you have monoid S and a (finite or infinite) collection of submonoids $S_1, S_2, \ldots$ of S (a submonoid is a subset of S that contains the identity element of S and itself forms a monoid under the operation of S). When we say that S is the direct sum $\oplus S_n = S_1 \oplus S_2 \oplus \cdots$ of these submonoids, we will mean that every nonidentity element of S can be written in a unique way (up to order of the factors) as a product of nonidentity elements from finitely many of the different submonoids. A good example to keep in mind is the counting numbers $S = \{1, 2, \ldots\}$, with the operation of multiplication. Let $\mathcal{P}$ denote the set of prime numbers, and for each $p \in \mathcal{P}$, let S_p be the submonoid $\{1, p, p^2, p^3, \ldots\}$ of S. The fact that each counting number factors uniquely into a product of prime factors says exactly that $S = \oplus_{p \in \mathcal{P}} S_p = S_2 \oplus S_3 \oplus S_5 \oplus \cdots$.

We begin by determining how to identify the primitive GPTs from their a-h coordinates.

PROPOSITION 1. *For $h \neq 0$, $[a, h]$ is primitive exactly when either*

1. *a is odd and $h = \pm q^2$ with q odd and* $\gcd(a, h) = q$, *or*
2. *a is even and $h = \pm 2q^2$ with* $\gcd(a, h) = 2q$.

Proof. Since $[a, h] = -[-a, -h]$, we may assume that $h > 0$. Suppose that $[a, h]$ is primitive. If $h = q^2$, then according to Corollary 1, $a = q(q + 2k)$ with $\gcd(2k, q) = 1$, so $\gcd(a, h) = q$. If $h = 2q^2$, then $a = 2q(q + k)$ with $\gcd(2q, k) = 1$, so $\gcd(a, h) = 2q$.

Conversely, suppose that $[a, h]$ is not primitive. If h is not of the form q^2 with q odd or $2q^2$, then neither condition holds. Suppose that $h = q^2$. Since the triple is not primitive, statement 1 of Theorem 1 shows that k and h are divisible by an odd prime p. Since $a = q(q + 2k)$, pq divides both a and h. This shows that $\gcd(a, h)$ must be greater than q. The case of $h = 2q^2$ is similar. ∎

Recall that if $[a, h]$ is a GPT and n is a nonzero integer, then $n[a, h] = [na, nh]$. Consequently, if a product of PTs is primitive, each factor must be primitive (although a product of PPTs need not be primitive, for example $(4, 3, 5) * (4, 3, 5) = 2(8, 15, 17)$). Beauregard and Suryanarayan [**4**] proved the following unique factorization theorem for the monoid $\mathcal{D}$.

THEOREM 5. *Let $[a, h] \in \mathcal{D}$ be primitive. Write a as $\pm 2^r p_1^{r_1} \cdots p_m^{r_m} q_1^{s_1} \cdots q_n^{s_n}$, where $r \geq 0$, all r_i and s_j are positive, and $\{p_1, \ldots, p_m, q_1, \ldots, q_n\}$ are distinct odd primes, with the q_j being the odd prime factors of a that are also factors of h. Then $[a, h]$ factors uniquely as $S_0 * P_0 * (\prod_{i=1}^m [p_i, 1]^{r_i}) * (\prod_{j=1}^n [q_j, q_j^2]^{s_j})$, where S_0 is one of the four GPTs $[\pm 1, \pm 1]$, and*

(i) $P_0 = [1, 1]$ *if h is odd,*

(ii) $P_0 = [2^r, 2]$ *if $h \equiv 2 \mod 4$, and*

(iii) $P_0 = [2^r, 2^{2r-1}]$ *if $h \equiv 0 \mod 4$.*

In the latter two cases, $r \geq 2$.

We will now use a-h coordinates to give a proof of this result. Our proof will not use Theorem 4. While Theorem 5 can be deduced as a corollary of Theorem 4, this does not seem to shorten the proof if one wants the precise information about how the form of P_0 depends on h. Theorem 4 can be deduced from Theorem 5 [**4**].

Proof. Factoring out S_0 allows us to assume that both a and h are positive. We first prove the existence of the factorization. Suppose first that a is odd; by Proposition 1, $h = q^2$ with q odd and $\gcd(a, h) = q$. So we can write $h = q_1^{2s_1} \cdots q_n^{2s_n}$ and $a = p_1^{r_1} \cdots p_m^{r_m} q_1^{s_1} \cdots q_n^{s_n}$, with all r_i and s_j positive, and $p_1, \ldots, p_m, q_1, \ldots, q_n$ distinct odd primes. This give the desired factorization with P_0 chosen as in (i).

Now suppose that a is even; by Proposition 1, $h = 2q^2$ with $\gcd(a, h) = 2q$. So we can write $h = 2^{2s_0+1} q_1^{2s_1} \cdots q_n^{2s_n}$ and $a = 2^r p_1^{r_1} \cdots p_m^{r_m} q_1^{s_1} \cdots q_n^{s_n}$. If $s_0 = 0$, then we obtain a factorization of $[a, h]$ with P_0 as in (ii). In this case, $r \geq 2$, since a factor of $[2, 2]$ would prevent $[a, h]$ from being primitive. If $s_0 > 0$, then since $\gcd(a, h) = 2^{s_0+1} q_1^{s_1} \cdots q_n^{s_n}$, we must have $r = s_0 + 1$ giving a factorization with P_0 as in (iii), with $r \geq 2$.

For the uniqueness of the factorization, we observe that the product of the first entries must be a, and the only way that the second entries can have product equal to h is for the factor of h that is a power of 2 to be paired with the factor 2^r of a, and for each of the $q_{s_i}^2$ factors of h to be paired with one of the q_{s_i} factors of a that appears in a term of the form $[q_{s_i}, q_{s_i}^2]$. ∎

COROLLARY 2. *Let $[a, h] \in \mathcal{D}$. Then $[a, h]$ can be written uniquely in the form $S_0 * [2^s, 2^t] * (\prod_{i=1}^m [p_i^{s_i}, p_i^{t_i}])$, where the p_i are distinct odd primes, $s, t \geq 0$, each $s_i, t_i \geq 0$ and $s_i + t_i > 0$, and S_0 is one of the four GPTs $[\pm 1, \pm 1]$. In this form, each $t_i \leq 2s_i$, and either $s = t = 0$ or $1 \leq t < 2s$.*

Proof. Write $[a, h]$ as $[N, N] * [a_1, h_1]$, where N is a positive integer and $[a_1, h_1]$ is primitive. Using the factorization for $[a_1, h_1]$ given in Theorem 5, we obtain a factorization for $[a, h]$ of the desired form. It is unique, since the product of the first entries of the factors is a and the product of the second entries is h. ∎

Now, we can develop the precise structure of the monoid $\mathcal{D}$. First, note that $\mathcal{D}$ is the union of two nonintersecting semigroups: $\mathcal{D}_0$, the set of $[0, h]$, and $\mathcal{D}_{\neq 0}$, the monoid consisting of the $[a, h]$ with $a \neq 0$. When $a = 0$, h must be even, so $\mathcal{D}_0$ is isomorphic to the semigroup $2\mathbb{Z} - \{0\}$ under multiplication. The rule $[0, h_1] * [a, h_2] = [0, h_1 h_2]$ shows exactly how to multiply an element of $\mathcal{D}_0$ by an element of $\mathcal{D}_{\neq 0}$, so to understand the multiplicative structure of $\mathcal{D}$, it remains only to understand $\mathcal{D}_{\neq 0}$. Let $\mathcal{A}$ be the

monoid consisting of the $[a, h]$ with a and h both positive. Since each $[a, h]$ in $\mathcal{D}_{\neq 0}$ can be written uniquely as $[\epsilon_1, \epsilon_2] * [a_1, h_1]$, with $[\epsilon_1, \epsilon_2] \in \{[\pm 1, \pm 1]\}$ and $[a_1, h_1] \in \mathcal{A}$, $\mathcal{D}_{\neq 0}$ is the direct sum $\{[\pm 1, \pm 1]\} \oplus \mathcal{A}$. So it remains only to understand $\mathcal{A}$. In the process, we will determine exactly which elements of $\mathcal{D}$ can be written as products of primitive GPTs.

Begin with an $[a, h]$ in $\mathcal{A}$. By Corollary 2, $[a, h]$ can be factored uniquely as $\prod_{i=1}^{m} [p_i^{s_i}, p_i^{t_i}]$, where the p_i are distinct primes and the exponents are all nonnegative, and for each i, $s_i + t_i > 0$ and $t_i \leq 2s_i$, and moreover if $p_i = 2$ then $1 \leq t_i < 2s_i$. So we can write $\mathcal{A}$ as the direct sum $\bigoplus_{p \in \mathcal{P}} \mathcal{A}_p$, where $\mathcal{P}$ is the set of primes and

1. For p an odd prime, $\mathcal{A}_p$ is the set of GPTs of the form $[p^s, p^t]$ with $s, t \geq 0$ and $t \leq 2s$.
2. $\mathcal{A}_2$ is the set of GPTs of the form $[2^s, 2^t]$, where $s, t \geq 0$ and either $s = t = 0$ or $1 \leq t < 2s$.

We will see that the $\mathcal{A}_p$ with p odd are rather easy to describe and are all essentially the same, while $\mathcal{A}_2$ is quite a bit more complicated.

We first analyze the $\mathcal{A}_p$ for an odd p. Since $t \leq 2s$, any element $[p^s, p^t]$ of $\mathcal{A}_p$ can be written as $[p, p]^u * [p, 1]^v * [p, p^2]^w$, with u, v, and w nonnegative and at least one of them positive. We identify $[p^s, p^t]$ with the vector (s, t), so that the operation becomes vector addition. This identifies $\mathcal{A}_p$ with the submonoid $\mathbb{M}$ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ generated by the vectors $(1, 1)$, $(1, 0)$, and $(1, 2)$. The latter two vectors generate a submonoid that we call $\mathcal{B}_p$; for each $(s, t) \in \mathcal{B}_p$, t is even.

The first coordinate system in FIGURE 5 shows a picture of $\mathcal{A}_p$, with the solid dots indicating the elements of $\mathcal{B}_p$. One sees, either by calculation or by noticing that in FIGURE 5, adding the vector $(1, 1)$ moves the solid dots to the open circles, that every element of $\mathcal{A}_p$ can be written uniquely as $[p, 1]^u * [p, p^2]^v * [p, p]^\epsilon$ with ϵ equal to 0 or 1, and an element lies in $\mathcal{B}_p$ if and only if $\epsilon = 0$, that is, when it has the form $[p^s, p^t]$ with t even. Thus $\mathcal{B}_p$ consists exactly of the elements of $\mathcal{A}_p$ that are products of PPTs.

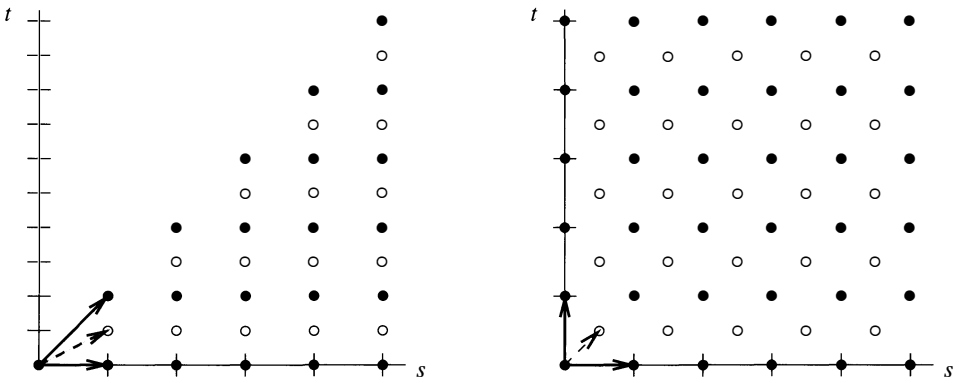


Figure 5 $\mathcal{A}_p$ and $\mathcal{B}_p$ for p an odd prime

Algebraically, $\mathcal{A}_p$ is generated as a semigroup by three generators $\gamma_1 = [p, 1]$, $\gamma_2 = [p, p^2]$, and $\gamma_3 = [p, p]$, subject to the relation that $\gamma_1 * \gamma_2 = \gamma_3 * \gamma_3$, and $\mathcal{B}_p$ is the submonoid generated by γ_1 and γ_2. In fact, $\mathcal{B}_p$ is isomorphic to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$. An explicit isomorphism is given by multiplication by the matrix

$$\begin{pmatrix} 1 & -1/2 \\ 0 & 1/2 \end{pmatrix}$$

(as usual, we regard (s, t) as a column vector and multiply on the left by this matrix). The second coordinate system of FIGURE 5 shows the result of multiplying the vectors of $\mathcal{A}_p$ by this matrix. This carries $\mathcal{B}_p$ to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$, and $\mathcal{A}_p - \mathcal{B}_p$ to the vectors of the form $(1/2, 1/2) + (s, t)$ for $(s, t) \in \mathcal{B}_p$.

Now we analyze $\mathcal{A}_2$. By Corollary 2, $\mathcal{A}_2$ consists of $[1, 1]$ and the $[2^s, 2^t]$ with $1 \leq t < 2s$. Again changing to vector notation, we identify $\mathcal{A}_2$ with the submonoid $\mathbb{M}_2$ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ consisting of $(0, 0)$ and all (s, t) with $1 \leq t < 2s$. There is no finite generating set for $\mathcal{A}_2$. For the angles of inclination of the nonzero vectors in the span of any finite subset of $\mathbb{M}_2$ are bounded away from 0, but 0 is a limit point for the set of angles of inclination of elements of M_2.

Define the submonoid $\mathcal{B}_2$ of $\mathcal{A}_2$ to consist of the products of primitive GPTs. Let $\mathcal{S}_2^+ = \{(s, 1) \mid s \geq 2\}$ and $\mathcal{S}_2^- = \{(s, 2s - 1) \mid s \geq 2\}$. Theorem 5 shows that $\mathcal{S}_2 = \{(0, 0)\} \cup \mathcal{S}_2^+ \cup \mathcal{S}_2^-$ is the collection of all primitive GPTs in $\mathcal{A}_2$, so $\mathcal{B}_2$ is the submonoid generated by $\mathcal{S}_2$. In a previous version of this article, we gave a proof that $\mathcal{B}_2$ contains all but finitely many elements of $\mathcal{A}_2$. We thank the referee for improvements that give the following sharper result.

THEOREM 6. *The set* $\mathcal{A}_2 - \mathcal{B}_2$ *consists of* (1, 1), (2, 2), (3, 2), (3, 3), (3, 4), (4, 3), (4, 5), (5, 3), (5, 5), *and* (5, 7)}; *these are exactly the PTs* $2^n(1, 0, 1)$ *for* $n = 1, 2, 3,$ *and* 5, $2(4, \pm 3, 5)$, $4(4, \pm 3, 5)$, *and* $4(8, \pm 15, 17)$.

Proof. In our proof, all variables will represent positive integers. First, consider the region L in FIGURE 6, which consists of all nonzero $(s, t) \in \mathcal{A}_2$ having $1 \leq t \leq s/2$. We claim that $L \subset \mathcal{B}_2$, as we will show by induction on t. If $t = 1$, then $(s, t) \in \mathcal{S}_2^+$. If $t > 1$, then $(s, t) = (2, 1) + (s - 2, t - 1)$, with $(s - 2, t - 1) \in L$. By the induction hypothesis, $(s - 2, t - 1) \in \mathcal{B}_2$, so $(s, t) \in \mathcal{B}_2$.

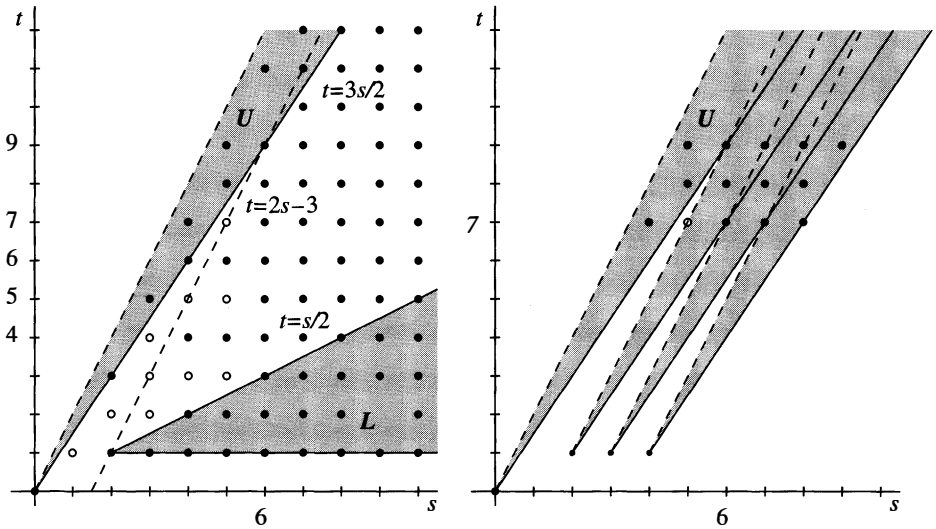


Figure 6 Finding $\mathcal{A}_2 - \mathcal{B}_2$

Next, we claim that $U \subset \mathcal{B}_2$, where, as shown in FIGURE 6, U is the set of (s, t) satisfying $3 \leq 3s/2 \leq t < 2s$. Let M be the matrix

$$\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}.$$

Notice that $M = M^{-1}$, and M carries integer lattice points to integer lattice points. As usual, thinking of vectors as column vectors when necessary, we have $M(s, 1) = (s, 2s - 1)$, so M interchanges the sets $\mathcal{S}_2^+$ and $\mathcal{S}_2^-$. Also, M interchanges the s-axis with the line $t = 2s$ and interchanges the line $t = s/2$ with the line $t = 3s/2$. That is, M interchanges the sets U and L. Since multiplication by M is a homomorphism with respect to vector addition, and every element of L is a sum of elements of $\mathcal{S}_2^+$, this shows that every element of U is a sum of elements of $\mathcal{S}_2^-$, so $U \subset \mathcal{B}_2$.

We note that

1. For $s \geq 4$, $(s, 4) = (s - 2, 1) + (2, 3) \in \mathcal{B}_2$.
2. For $s \geq 6$, $(s, 5) = (s - 2, 4) + (2, 1) \in \mathcal{B}_2$.
3. For $s \geq 5$, $(s, 6) = (3, 5) + (s - 3, 1) \in \mathcal{B}_2$.

Now, write $(s, t) + U$ to mean the set of all points of the form $(s, t) + (u, v)$ with $(u, v) \in U$. The second graph in FIGURE 6 shows the sets $(2, 1) + U$, $(3, 1) + U$, and $(4, 1) + U$, and makes it clear that the union of all $(n, 1) + U$ for $n \geq 2$ contains all (s, t) with $s \geq 6$ and $t \geq 7$. Since each $(n, 1) + U \subset \mathcal{B}_2$, all of these points are in $\mathcal{B}_2$.

Combining the observations made so far shows that all the solid dots in the first graph in FIGURE 6 are in $\mathcal{B}_2$, leaving only the points listed in the statement of the theorem, shown as hollow dots, as candidates for the points of $\mathcal{A}_2 - \mathcal{B}_2$.

To check that these ten points are not in $\mathcal{B}_2$, we induct on s. Each element of $\mathcal{S}_2$ other than $(0, 0)$ has s-coordinate at least 2, so $(1, 1)$ is not in $\mathcal{B}_2$. Since $(2, 2)$ is not one of the primitives $(2, 1)$ or $(2, 3)$, it is not in $\mathcal{B}_2$. To be in $\mathcal{B}_2$, each of $(3, 2)$, $(3, 3)$ and $(3, 4)$ would have to be $(2, 1) + (1, t)$ or $(2, 3) + (1, t)$, which is impossible since no $(1, t)$ is primitive. Each of $(4, 3)$ and $(4, 5)$ would have to be either $(2, 1) + (2, t)$ or $(2, 3) + (2, t)$, for $t = 1$ or $t = 3$, again giving no posssibilites. Finally, $(5, 3)$, $(5, 5)$, or $(5, 7)$ would have to be $(2, 1) + (3, t)$ or $(2, 3) + (3, t)$, for $t = 1$ or $t = 5$. ■

As was the case for $\mathcal{A}_p$, multiplication by the matrix

$$\begin{pmatrix} 1 & -1/2 \\ 0 & 1/2 \end{pmatrix}$$

clarifies the picture. FIGURE 7 shows the result of multiplying the vectors of $\mathcal{A}_2$ by this matrix. The nonzero primitives are carried to the points $(n + 1/2, 1/2)$ and $(1/2, n + 1/2)$ for $n \geq 1$.

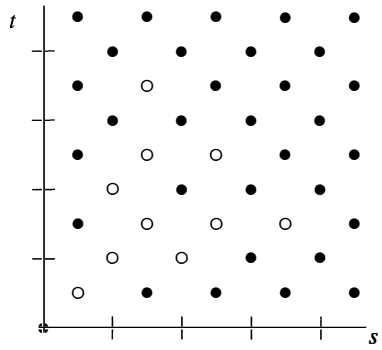


Figure 7 A better view of $\mathcal{A}_2$ and $\mathcal{B}_2$

We still need to identify which elements of $\mathcal{D}_0$ are products of primitives. We denote this subsemigroup by $\mathcal{B}_0$. For any product of elements of $\mathcal{D}$ that lies in $\mathcal{D}_0$, one of the

factors must have $a = 0$. The only primitives in $\mathcal{D}_0$ are $[0, \pm 2]$, so the only products of primitive elements from $\mathcal{D}_0$ are the $[0, \pm 2^n]$ with $n \geq 1$. The h-coordinates of the other primitive factors, up to sign, all have the form q^2 with q odd, or $2q^2$ with $q \neq 0$. So the h-coordinate of the product must have the form $\pm Q^2$ with Q even, or $\pm 2Q^2$, and any number of this form can be achieved.

Summarizing, we have the complete monoid structure.

THEOREM 7. *The Beauregard-Suryanarayan monoid $\mathcal{D}$ is a disjoint union $\mathcal{D}_0 \cup \mathcal{D}_{\neq 0}$, where $\mathcal{D}_0$ consists of all $[0, h]$ with h even, and is isomorphic to $2\mathbb{Z} - \{0\}$. There is a direct sum decomposition*

$$\mathcal{D}_{\neq 0} = \{[\pm 1, \pm 1]\} \oplus \mathcal{A}_2 \oplus \left(\bigoplus_{p \in \mathcal{P} - \{2\}} \mathcal{A}_p \right),$$

with each $\mathcal{A}_p$ isomorphic to the 3-generator monoid $\mathbb{M}$, and $\mathcal{A}_2$ isomorphic to the non-finitely-generated monoid $\mathbb{M}_2$. The submonoid of products of primitive GPTs is a disjoint union $\mathcal{B}_0 \cup \mathcal{B}_{\neq 0}$, where $\mathcal{B}_0$ consists of all $[0, h]$ with h of the form $\pm q^2$ with q even, or $\pm 2q^2$, and

$$\mathcal{B}_{\neq 0} = \left\{[\pm 1, \pm 1]\right\} \oplus \mathcal{B}_2 \oplus \left(\bigoplus_{p \in \mathcal{P} - \{2\}} \mathcal{B}_p \right),$$

where each $\mathcal{B}_p$ consists of the $[p^s, p^t]$ in $\mathcal{A}_p$ with t even, and $\mathcal{B}_2$ consists of all but the ten elements of $\mathcal{A}_2$ specified in Theorem 6.

The e-operation

In this final section, we adapt our approach to the Beauregard-Suryanarayan operation to develop a new operation on GPTs (with $h \neq 0$), which is multiplicative with respect to e and to h. We will see that as with the Beauregard-Suryanarayan operation, the group obtained by projectivization can be naturally identified with $\{1, -1\} \times \mathbb{Q}$, but this time the subgroup corresponding to $\{1\} \times \mathbb{Q}_{>0}$ *is exactly the set of PPTs.*

Since $e = kd$, Theorem 1 shows that e-h coordinates on the set $\mathcal{D}$ of GPTs with $h \neq 0$ can be defined by putting

$$\langle e, h \rangle = \left(h + e, e + \frac{e^2}{2h}, h + e + \frac{e^2}{2h} \right).$$

Theorem 1 and Lemma 1 show that $\langle e, h \rangle$ represents a GPT exactly when h and e are integers such that $h \neq 0$ and $2h$ divides e^2, and $\langle e, h \rangle$ is a PT exactly when both e and h are positive. Some examples are:

1. $\langle 2, 1 \rangle = (3, 4, 5)$, $\langle 2, 2 \rangle = (4, 3, 5)$, $\langle 2, -2 \rangle = (0, 1, -1)$.
2. $\langle 2p, 1 \rangle = (1 + 2p, 2p + 2p^2, 1 + 2p + 2p^2)$.
3. $\langle 2p, 2 \rangle = (2 + 2p, 2p + p^2, 2 + 2p + p^2)$.
4. $\langle 2q, q^2 \rangle = (q^2 + 2q, 2q + 2, q^2 + 2q + 2)$.
5. $\langle 2^s, 2^{2s-1} \rangle = (2^s + 2^{2s-1}, 1 + 2^s, 1 + 2^s + 2^{2s-1})$ with $s \geq 1$.

The relation between e-h coordinates and a-h coordinates is just that $\langle e, h \rangle = [e + h, h]$, so the condition to identify primitive GPTs is exactly that of Proposition 1:

PROPOSITION 2. *For $h \neq 0$, $\langle e, h\rangle$ is primitive exactly when either*

1. $h = \pm q^2$ *with q odd and* $\gcd(e, h) = q$, *or*
2. $h = \pm 2q^2$, *and* $\gcd(e, h) = 2q$.

We define an operation by the simple rule

$$\langle e_1, h_1\rangle \langle e_2, h_2\rangle = \langle e_1 e_2, h_1 h_2\rangle$$

and call it the *e-operation.* Notice that $\langle e_1 e_2, h_1 h_2\rangle$ does represent a GPT, since if $2h_1 \mid e_1^2$ and $2h_2 \mid e_2^2$, then $2h_1 h_2 \mid (e_1 e_2)^2$. In (a, b, c)-coordinates (obviously the wrong ones for viewing it), the operation takes the form

$$\begin{aligned}(a_1, b_1, c_1)(a_2, b_2, c_2) = \\ (a_1a_2 + a_1b_2 - a_1c_2 + b_1a_2 + 2b_1b_2 - 2b_1c_2 - c_1a_2 - 2c_1b_2 + 2c_1c_2,\\ 3a_1a_2 + a_1b_2 - 3a_1c_2 + b_1a_2 + b_1b_2 - b_1c_2 - 3c_1a_2 - c_1b_2 + 3c_1c_2,\\ 3a_1a_2 + a_1b_2 - 3a_1c_2 + b_1a_2 + 2b_1b_2 - 2b_1c_2 - 3c_1a_2 - 2c_1b_2 + 4c_1c_2),\end{aligned}$$

and in a-h coordinates it is $[a_1, h_1][a_2, h_2] = [a_1a_2 - a_1h_2 - a_2h_1 + 2h_1h_2, h_1h_2]$. Here are a couple of sample calculations.

$$\begin{aligned}(3, 4, 5)\,(3, 4, 5) &= \langle 2, 1\rangle \langle 2, 1\rangle \\ &= \langle 4, 1\rangle = (5, 12, 13)\\ (4, 3, 5)\,(a, b, c) &= \langle 2, 2\rangle \langle a + b - c, c - b\rangle \\ &= \langle 2(a + b - c), 2(c - b)\rangle = (2a, 2b, 2c)\end{aligned}$$

For $\langle e, h\rangle = (a, b, c)$ and any nonzero integer n, we have $n\langle e, h\rangle = (na, nb, nc) = \langle ne, nh\rangle$, and we will declare all these equivalent. Denote the set of equivalence classes with $h \neq 0$ by $\mathcal{E}$.

THEOREM 8. *Define $\phi: \mathcal{E} \to \{1, -1\} \times \mathbb{Q}$ by sending $\langle e, h\rangle$ to $(\sigma(h), e/h)$, where $\sigma(h) = 1$ if h is positive and is -1 if h is negative. Then ϕ is an isomorphism.*

Proof. As in Theorem 4, it is straightforward to check that ϕ is a well-defined homomorphism. It is surjective, since $\phi(\pm\langle 2, 2\rangle) = (\pm 1, 1)$, $\phi(\pm\langle 2, -2\rangle) = (\pm 1, -1)$, $\phi(\langle 0, 1\rangle) = (1, 0)$, $\phi(\langle 2, 1\rangle) = (1, 2)$, $\phi(\langle 4, 8\rangle) = (1, 1/2)$, and $\phi(\langle 4, 8\rangle\langle 2q, 1\rangle) = (1, q)$ and $\phi(\langle 4, 8\rangle\langle 2q, q^2\rangle) = (1, 1/q)$, when q is an odd prime. For injectivity, suppose that $\phi(\langle e_1, h_1\rangle) = \phi(\langle e_2, h_2\rangle)$. Then h_1 and h_2 have the same sign, so replacing each $\langle e_i, h_i\rangle$ by $\langle -e_i, -h_i\rangle$ if necessary, we may assume that both h_1 and h_2 are positive. Since

$$\frac{1}{h}\langle e, h\rangle = \left(1 + \frac{e}{h}, \frac{e}{h} + \frac{1}{2}\left(\frac{e}{h}\right)^2, 1 + \frac{e}{h} + \frac{1}{2}\left(\frac{e}{h}\right)^2\right),$$

we have $h_2\langle e_1, h_1\rangle = h_1\langle e_2, h_2\rangle$. Thus $\langle e_1, h_1\rangle$ and $\langle e_2, h_2\rangle$ are projectively equivalent and represent the same element of $\mathcal{E}$. ∎

Under this isomorphism, the PPTs correspond exactly to $\mathbb{Q}_{>0}$, so they form an abelian group free on the generators $\{\langle 2, 1\rangle\} \cup \{\langle 2p, 2\rangle \mid p \text{ is prime}\}$. It is also free on the set of height-1 PPTs $\{\langle 2, 1\rangle\} \cup \{\langle 2p, 1\rangle \mid p \text{ is prime}\}$.

Unlike the Beauregard-Suryanarayan operation, the e-operation is not well-behaved at the level of PTs. For example, it has no identity element, and appears to have poor

factorization properties, since no GPT $\langle e, h \rangle$ with $e \equiv 2 \mod 4$ can be factored into a product of two GPTs. But perhaps there is still some nice structure hiding there.

Acknowledgment. The author was supported in part by NSF grant DMS-0102463. He thanks the referees for many suggestions that improved this article.

REFERENCES

1. R. Amato, On the determination of Pythagorean triples, (Italian, English summary) *Atti Soc. Peloritana Sci. Fis. Mat. Natur.* **27** (1981), 3–8.
2. P. J. Arpaia, A generating property of Pythagorean triples, this MAGAZINE **44** (1971), 26–27.
3. F. J. M. Barning, On Pythagorean and quasi-Pythagorean triangles and a generation process with the help of unimodular matrices, (Dutch) *Math. Centrum Amsterdam Afd. Zuivere Wisk,* ZW-011 (1963) 37 pp.
4. R. Beauregard and E. Suryanarayan, Pythagorean triples: the hyperbolic view, *College Math. J.* **27** (1996), 170–181.
5. H. Becker, http://home.foni.net/~heinzbecker/pythagoras.html
6. J. Buddenhagen, C. Ford, and M. May, Nice cubic polynomials, Pythagorean triples, and the law of cosines, this MAGAZINE **65** (1992), 244–249.
7. B. Dawson, The ring of Pythagorean triples, *Missouri J. Math. Sci.* **6** (1994), 72–77.
8. E. Eckert, The group of primitive Pythagorean triangles, this MAGAZINE **57** (1984), 22–27.
9. A. Grytczuk, Note on a Pythagorean ring, *Missouri J. Math. Sci.* **9** (1997), 83–89.
10. J. Gollnick, H. Scheid, J. Zöllner, Rekursive Erzeugung der primitiven pythagoreischen Tripel, (German) [Recursive generation of primitive Pythagorean triples], *Math. Semesterber.* **39** (1992), 85–88.
11. A. Hall, Genealogy of Pythagorean triads, *Mathematical Gazette* **54:390** (1970), 377–379.
12. E. Hlawka, Pythagorean triples, in *Number Theory* (ed. R. P. Bambaugh, V. C. Dumir, and R. J. Hans-Gill), in series *Trends in Mathematics*, Birkhäuser, Basel (2000), 141–155.
13. J. Jaeger, Pythagorean number sets (Danish, English summary), *Nordisk Mat. Tidskr.* **24** (1976), 56–60, 75.
14. T. A. Jenkyns and D. McCarthy, Integers in Pythagorean triples, *Bull. Inst. Combin. Appl.* **4** (1992), 53–57.
15. Kanga, A. R., The family tree of Pythagorean triples, *Bull. Inst. Math. Appl.* **26** (1990), 15–17.
16. H. Klostergaard, Tabulating all Pythagorean triples, this MAGAZINE **51** (1978), 226–227.
17. E. Kristensen, Pythagorean number sets and orthonormal matrices, (Danish, English summary) *Nordisk Mat. Tidskr.* **24** (1976), 111–122, 135.
18. D. McCullough and E. Wade, Recursive enumeration of Pythagorean triples, *College Math. J.* **34** (2003), 107-111.
19. L. Palmer, M. Ahuja, and M. Tikoo, Finding Pythagorean triple preserving matrices, *Missouri J. Math. Sci.* **10** (1998), 99–105.
20. ———, Constructing Pythagorean triple preserving matrices, *Missouri J. Math. Sci.* **10** (1998), 159–168.
21. Préau, Paul, Un graphe ternaire associé à l'équation $X^2 + Y^2 = Z^2$, (French, English summary) [A ternary graph associated with the equation $X^2 + Y^2 = Z^2$], *C. R. Acad. Sci. Paris Sér. I Math.* **319** (1994), 665–668.
22. O. Taussky, Sums of squares, *Am. Math. Monthly* **77** (1970), 805–830.
23. M. G. Teigan and D. W. Hadwin, On generating Pythagorean triples, *Amer. Math. Monthly* **78** (1971), 378–379.
24. P. W. Wade and W. R. Wade, Recursions that produce Pythagorean triples, *College Math. J.* **31** (2000), 98–101.
25. M. Wójtowicz, Algebraic structures of some sets of Pythagorean triples, I, *Missouri J. Math. Sci.* **12** (2000), 31–35.
26. ———, Algebraic structures of some sets of Pythagorean triples, II, *Missouri J. Math. Sci.* **13** (2001), 17–23.

A Note from the Problems Editor

John Cobb and Martin Tangora each noted that there is an even quicker solution to Quickie 943 (October 2004). Because the metric space (X, d) is compact, $d(x, y)$ assumes its maximum on $X \times X$. Thus $d(f(x), f(y)) > d(x, y)$ cannot be true for every pair (x, y) with $x \neq y$. Hence X must consist of a single point.

NOTES

Hidden Group Structure

RUTH I. BERGER
Luther College
Decorah, IA 52101
bergerr@luther.edu

You may have seen the problem: "*Show that the set* $S = \{5, 15, 25, 35\}$ *is a group under multiplication modulo 40*," in Gallian's well known text book [**1**]. This is quite puzzling to beginning students in abstract algebra, especially since there is no obvious identity. Even after 25 has been identified as the identity element, the question of determining inverses requires some thought. The astute observer notices that the above set S is in fact closely related to $U(8) = \{1, 3, 5, 7\}$, which is a group under multiplication modulo 8. All elements and the modulus have been multiplied by 5. But the fact that $S = 5 \cdot U(8)$ does not explain its group structure since then one would expect $5 \cdot 1$ to be the identity element, not $5 \cdot 5$.

Before we proceed to investigate this intriguing connection we need to introduce some notation. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ be the ring of integers modulo n and consider $U(n)$, the group of units (invertible elements) of $\mathbb{Z}_n$, which is a group under multiplication modulo n. In this paper, we will investigate whether, for any $k \in U(n)$, the set $S_k(n) = k \cdot U(n) = \{k \cdot g \mid g \in U(n)\}$ is a group under multiplication modulo kn. For example, from $U(8) = \{1, 3, 5, 7\}$ under multiplication modulo 8 we obtain

$S_3(8) = \{3, 9, 15, 21\}$ under multiplication modulo 24,
$S_5(8) = \{5, 15, 25, 35\}$ under multiplication modulo 40, and
$S_7(8) = \{7, 21, 35, 49\}$ under multiplication modulo 56.

You can check that these are in fact groups! Some computation reveals that their respective identity elements are 9, 25, and 49. Each element of these groups turns out to be its own inverse, so each of these groups has the same structure as $U(8)$; that is, $S_k(8)$ is isomorphic to $U(8)$. This may not seem very surprising, after all, the sets were obtained from $U(8)$. But something more subtle is going on here, because the map $f : U(n) \to S_k(n)$ given by $f(x) = k \cdot x$ is not a group homomorphism! One way to see this is to observe that $f(1) = k$ is not the identity element of $S_k(8)$. So, is there any way to predict that 25 will act as the identity in $S_5(8)$? Why is it that in $S_k(8)$ the respective identity elements are all squares, namely k^2? Will $S_k(n)$ always be a group under multiplication modulo kn? And if so, will the group $S_k(n)$ always be isomorphic to $U(n)$?

When looking for sets of integers that are groups under multiplication modulo kn one would usually look for subgroups of $U(kn)$, the group of units of the ring $\mathbb{Z}_{kn}$. But note that even though $S_k(n)$ is a subset of $\mathbb{Z}_{kn}$, the intersection of $S_k(n)$ and $U(kn)$ is empty, since all elements of $S_k(n)$ are multiples of k and therefore not invertible. This is what makes it quite surprising that $S_k(n)$ turns out to be a group under multiplication modulo kn.

$S_k(n)$ is a group We are working with two different moduli: mod n in $U(n)$ and mod kn in $S_k(n)$, and we must therefore be very careful when using the words *identity*

and *inverse*. We use the following notation to keep the two situations separate: The identity in $U(n)$ is 1, the identity in $S_k(n)$ will be denoted by E. For $x \in U(n)$, let x' denote its inverse modulo n; that is $x \cdot x' \equiv 1 \bmod n$. For $X \in S_k(n)$ we will denote its inverse by X^{-1}; that is $X \cdot X^{-1} \equiv E \bmod kn$. Note that when working modulo kn the element kk' is not 1. That is, $kk' \equiv 1 \bmod n$ but $kk' \not\equiv 1 \bmod kn$.

We will use of the following easy fact from modular arithmetic:

FACT 1. *Let $a, b, c, d \in \mathbb{Z}$. If $ad \equiv bd \bmod cd$ then $a \equiv b \bmod c$.*

THEOREM. *The set $S_k(n) := \{k \cdot g \mid g \in U(n)\}$ is a group under multiplication modulo kn, with identity element $E = kk'$.*

Proof.

(a) *Associativity* is inherited from the ring $\mathbb{Z}_{kn}$.

(b) *Closure:* Let kx and ky be elements of $S_k(n)$. Then $kx \cdot ky = k(kxy)$ and since k, x, and y are in $U(n)$, so is kxy; this shows that $(kx \cdot ky)$ is an element of $\{k \cdot g \mid g \in U(n)\} = S_k(n)$. Hence $S_k(n)$ is *closed* under multiplication modulo kn.

(c) *Identity:* We are looking for $E \in S_k(n)$ such that, for all $x \in U(n)$, we have $kx \cdot E \equiv kx \bmod kn$. By the above Fact 1 from modular arithmetic, it follows that $Ex \equiv x \bmod n$, and since x is an element of $U(n)$, we obtain $E \equiv 1 \bmod n$. The E in $S_k(n)$ that we are seek must have the form $E = kr$ for some $r \in U(n)$. From $k \cdot r \equiv 1 \bmod n$, we see that $r = k'$, the inverse of k in $U(n)$. Hence $E = kk'$ should be the identity element of $S_k(n)$. We can check this directly: $kx \cdot kk' = k(xkk') \equiv kx \bmod kn$, where in the last step we used $xkk' \equiv x \bmod n$.

(d) *Inverses:* Let $kx \in S_k(n)$. We are looking for $ky \in S_k(n)$ with $kx \cdot ky = E$ in $S_k(n)$, that is modulo kn. Applying the above Fact 1 to $kx \cdot ky \equiv kk' \bmod kn$, we see that $xky \equiv k' \bmod n$. Hence $ky \equiv x'k' \bmod n$, where x' is the inverse of x in $U(n)$, and therefore $y \equiv k'x'k' \bmod n$. This shows that $k \cdot k'x'k'$ should be the inverse of kx in $S_k(n)$. We can check this directly: $kk'x'k' \cdot kx = kk' \cdot (kk'xx') \equiv kk' = E \bmod kn$, here we used $kk'xx' \equiv 1 \bmod n$. ∎

Examples Let us reconsider the map $f : U(n) \to S_k(n)$ given by $f(x) = k \cdot x$. We have $f(k') = kk' = E$, so k' is the element of $U(n)$ that will map to the identity in $S_k(n)$. In the special case where $k = k'$ in $U(n)$, this gives $E = k^2$, which explains our observation about the identity in $S_k(8)$ being a square.

For $x \in U(n)$, which element will map to the inverse of $f(x)$ in $S_k(n)$? From the above: $k'x'k'$ will be that element. That is, $[f(x)]^{-1} = [kx]^{-1} = k \cdot k'x'k' = f(k'x'k')$. In the special case where $k = k'$ in $U(n)$ this simplifies to: $f(x') = [f(x)]^{-1}$, so the map f at least preserves inverses. In the case where $k \neq k'$ in $U(n)$ the group structure of $S_k(n)$ is more mysterious.

Let's examine $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15, where both types of k are available. The elements 4, 11, and 14 are their own inverses, while (2, 8) and (7, 13) are pairs of inverses.

For $k = 4$, we are in the case where k and k' are the same. We have $S_4(15) = 4 \cdot U(15) = \{4, 8, 16, 28, 32, 44, 52, 56\}$ under multiplication modulo 60. Here $E = f(4') = f(4) = 16$ is the identity element, $f(1) = 4$, $f(11) = 44$, $f(14) = 56$ are their own inverses, and ($f(2) = 8$, $f(8) = 32$) and ($f(7) = 28$, $f(13) = 52$) are pairs of inverses.

For $k = 7$, we are in the more interesting case where k is different from k'. We have $S_7(15) = 7 \cdot U(15) = \{7, 14, 28, 49, 56, 77, 91, 98\}$ under multiplication modulo 105. Here $E = f(7') = f(13) = 91$ is the identity element (not a square!), some computation shows that 14, 49, and 56 are their own inverses, and that (7, 28) and (77, 98) are

pairs of inverses. Note that $f(2) = 14$, with $14 = 14^{-1}$ in $S_7(15)$, but $2 \neq 2' \in U(15)$. How can one look at an element of $U(n)$ and predict its role in the group $S_k(n)$?

A group homomorphism Let's look at a different map, one that is a group homomorphism; that is, one that does preserve group structure.

For $x \in U(n)$ let $\Phi(x) := kk' \cdot x \bmod kn$.

To determine the image set of this map we first recall a fact from group theory:

FACT 2. *Let G be a group and $h \in G$ then $\{hg \mid g \in G\} = G$, since the map $g \mapsto hg$ has an inverse map.*

In particular, for $k \in U(n)$ this shows that $S_k(n) = k \cdot U(n) \equiv U(n) \bmod n$. That is, when the elements of $S_k(n)$ are reduced mod n we obtain the original set $U(n)$. They are equal as sets, but of course all the elements are shuffled around!

We can now examine the image of Φ: $Im(\Phi) = \{(kk' \cdot x) \bmod kn \mid x \in U(n)\} = \{k \cdot (k'x) \bmod kn \mid x \in U(n)\} = \{k \cdot y \bmod kn \mid y \in U(n)\} = k \cdot U(n) = S_k(n)$.

Therefore the map Φ takes $U(n)$ onto $S_k(n)$. Furthermore, Φ is a homomorphism because kk' is idempotent under multiplication modulo kn:

$$\Phi(x) \cdot \Phi(y) = kk'x \cdot kk'y \equiv k \cdot k'x(kk')y \equiv kk'xy = \Phi(xy) \bmod kn$$

where we reduced the $k'x(kk')y$ part modulo n, using $kk' \equiv 1 \bmod n$.

Note that even though kk' is the identity in $S_k(n)$, for $x \in U(n)$ the element xkk' *cannot* be simplified to $x \bmod kn$, unless x happens to be an element of $S_k(n)$.

Even though the existence of the isomorphism Φ shows that $S_k(n)$ has the same group structure as $U(n)$, in practice this is a very cumbersome way to see what is going on. An easier way to establish that $S_k(n)$ is isomorphic to $U(n)$ is to look at the map backwards. Since we have already established that $S_k(n)$ is a group under multiplication modulo kn, we can just consider the map that reduces each element of $S_k(n)$ modulo n. Its image turns out to be $U(n)$ by the above Fact 2. We have $\Phi(x) = kk'x \equiv x \bmod n$, since $kk' \equiv 1 \bmod n$, so the homomorphism that reduces $S_k(n)$ modulo n is in fact the inverse of Φ. This reduction mod n isomorphism is the easiest way to see the correspondence of elements from the group $S_k(n)$ to the group $U(n)$.

Consider the example of $S_7(15)$ from above:

$S_7(15) = \{7, 14, 28, 49, 56, 77, 91, 98\}$ under multiplication modulo 105.

Reducing the elements modulo 15, but writing the elements in the same order, gives

$$\{7, 14, 13, 4, 11, 2, 1, 8\} = U(15).$$

From this we see immediately (now that we know what is going on!) that 91 is the element corresponding to 1, that is, the identity element of $S_7(15)$. The other aspects of group structure, such as (77, 98) being a pair of inverses, or $77 \cdot 28 \equiv 56 \bmod 105$ is also clear now by observing their respective pre-images: (2, 8) is a pair of inverses in $U(15)$ and $2 \cdot 13 \equiv 11 \bmod 15$.

Conclusion You can now easily produce your own examples. Start with any positive integer n and any $k \in U(n)$. Compute $S_k(n) = k \cdot U(n)$, but do not reduce since this is to be considered modulo kn. Now reduce every element of $S_k(n)$ modulo n to obtain the re-shuffled $U(n)$ that reveals the group structure of $S_k(n)$.

To hide the original group structure even more, you can start with a subgroup G of $U(n)$. Either apply Φ by multiplying all elements of G by kk' and then reduce modulo kn; or look up the pre-images of G in the mod n reduction of $S_k(n)$. For example, from above we have $S_7(15) \cong U(15)$ with the following correspondence:

$S_7(15) \bmod 105$:	7	14	28	49	56	77	91	98
$U(15) \bmod 15$:	7	14	13	4	11	2	1	8

The subgroup $G = \{1, 11\}$ of $U(15)$ gives the subgroup $\Phi(G) = \{91, 56\}$ of $S_7(15)$. The subgroup $G = \{1, 2, 4, 8\}$ gives $\Phi(G) = \{91, 77, 98, 49\}$; and $G = \{1, 4, 11, 14\}$ gives $\Phi(G) = \{91, 49, 56, 14\}$. All of these $\Phi(G)$ are groups under multiplication modulo 105. Who would ever have guessed that! By using subgroups, the fact that these examples were obtained from $U(15)$ is no longer obvious.

Another interesting challenge might be to produce sets that are groups under multiplication modulo 2005. Since $2005 = 5 \cdot 401$, we can take $k = 5$, $n = 401$ and consider $S_5(401)$ under multiplication modulo 2005. The inverse of 5 in $U(401)$ is $k' = 321$, hence the identity in $S_5(141)$ will be $E = 5 \cdot 321 = 1605$. And any subgroup of $U(401)$ will produce a subgroup of $S_5(141)$. Consider $G = \{39, 318, 372, 72, 1\}$, the cyclic subgroup of $U(401)$ generated by 39. Multiply each element by 1605 then reduce modulo 2005, to obtain a group under multiplication modulo 2005: $\Phi(G) = \{440, 1120, 1575, 1275, 1605\}$. This is, of course, a cyclic group generated by $\Phi(39) = 440$.

Robin McLean [**2**] takes a different approach to these results. He also points out that one can pick any positive composite integer and produce a group that has this integer as its identity element. This can be done by observing $E \equiv 1 \bmod (E - 1)$. For example, if we want $E = 123$, consider $n = 122$. Since $E = 123 = 3 \cdot 41$, we can take $k = 3$, with inverse $k' = 41$ in $U(122)$. In $S_3(122)$ the identity element (mod $3 \cdot 122$) will be $E = kk' = 123$. Of course $S_3(122)$ has 60 elements, just like $U(122)$, but remember that any of its subgroups will also have 123 as identity element. For example: $\{123, 135, 291\}$ is a group under multiplication mod 366. Have fun producing your own examples!

REFERENCES

1. Joe Gallian, *Contemporary Abstract Algebra*, 5th ed., Houghton Mifflin (2002), p. 54.
2. Robin McLean, Groups in Modular Arithmetic, *Math. Gaz.*, **62** (1978), 94–104.

The St. Basil's Cake Problem

CHRISTINA SAVVIDOU
Department of Mathematics and Statistics
University of Cyprus
P.O. Box 20537
CY 1678 Nicosia
CYPRUS
ms01sc1@ucy.ac.cy

Perhaps the most popular cake in the Greek world during the Christmas period is not any well-known Christmas cake, but rather a cake called the St. Basil's cake. (St. Basil is commemorated by the Greek Orthodox Church on the first of January.) The cake is prepared using simple ingredients like flour, eggs, and orange juice, but also contains a coin wrapped in aluminum foil. When the cake is taken out of the oven, nobody knows where the coin is. With the arrival of the new year, this circular cake is cut (with a knife) into sectors of the circle. Each member of the family takes a sector and starts slowly and carefully eating his or her piece. The one who finds the coin, according to tradition, is considered to be the luckiest of the new year. However, sometimes, while

the cake is being cut into sectors, the knife hits the coin. This event happens quite often, and therefore it might be of interest to calculate its probability. Let's call this problem the *St. Basil's cake problem.*

Mathematical formulation First of all, observe that under the assumption that the coin is parallel to the base of the cake, the problem is equivalent to the following: A circle in the plane is divided into sectors. A coin is dropped at random on a circle, in a certain sense that we will clarify. We would like to calculate the probability that the coin is contained entirely in any one of the sectors.

The problem reminds us of the well known *Buffon's needle problem*, and in fact it might be considered as an extension or a variant of that. Let us very briefly describe the problem of the needle of Buffon. Consider a needle of length l that is dropped at random on a set of equidistant parallel lines that are d units apart, with $l < d$. What is the probability of an intersection? Uspenski [**2**] proved that this probability is $2l/\pi d$. His proof is a little bit complicated; a simpler proof is presented in Solomon [**1**], who also gives further details and various extensions and generalizations.

Solution Let us suppose that we have a circle of radius R^*, which is divided into $2n$ sectors with central angle π/n, and a coin with radius R_c. We must obviously assume that $R_c < R^*$. The coin is dropped at random on the circle by selecting a radius at random and locating the coin randomly along that radius.

The parameters that define the coin's position involve a vector from the center of the cake to the center of the coin. The length of this vector is r, and ϕ is the angle it makes with the closest cut of the circle. Then we can safely assume that r and ϕ are independent random variables. If the distance r is greater than $R^* - R_c$, then the coin would be partially outside of the circle. Thus, $r < R \equiv R^* - R_c$. The way we located the coin leads us to assume that r follows the uniform distribution on the interval $(0, R)$ and that ϕ follows the uniform distribution on the interval $(0, \pi/2n)$.

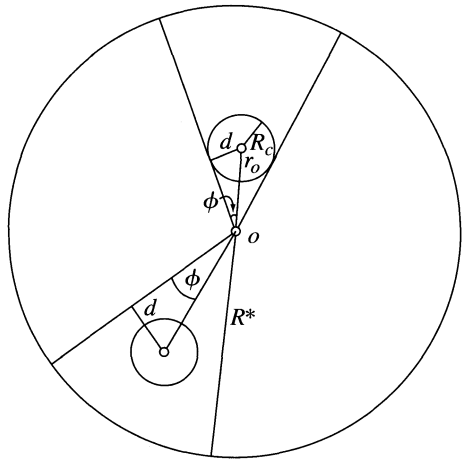


Figure 1 Locating the coin

Let d denote the distance of the center of the coin from the closest radius. As it can be seen in FIGURE 1, the coin is contained entirely in a sector if $r > r_0$, where r_0 satisfies the equation

$$\sin\left(\frac{\pi}{2n}\right) = \frac{R_c}{r_0}, \quad \text{that is,} \quad r_0 = \frac{R_c}{\sin(\pi/2n)}$$

and $d > R_c$, with the condition on d being equivalent to $r\sin\phi > R_c$, that is, $\phi > \arcsin(R_c/r)$.

Remark. We must assume that $R > r_0$ or equivalently, that $R\sin(\pi/2n) > R_c$, for otherwise the probability of an intersection is 1.

The probability that the coin is contained entirely in a sector is

$$\begin{aligned} P\big(r > r_0, \phi > \arcsin(R_c/r)\big) &= \int_{r_0}^{R} \int_{\arcsin(R_c/r)}^{\pi/2n} \frac{1}{R} \cdot \frac{1}{\pi/2n}\, d\phi\, dr \\ &= \int_{r_0}^{R} \left(\frac{1}{R} - \frac{2n}{\pi R}\arcsin(R_c/r)\right) dr \\ &= \frac{r}{R}\Big|_{r_0}^{R} - \int_{r_0}^{R} \frac{2n}{\pi R}\arcsin(R_c/r)\, dr \\ &= 1 - \frac{R_c}{R\sin(\pi/2n)} - \frac{2n}{\pi R}\int_{r_0}^{R} \arcsin(R_c/r)\, dr \\ &= 1 - \frac{R_c}{R\sin(\pi/2n)} - \frac{2n}{\pi R} I, \end{aligned} \tag{1}$$

where we have used I as a shorthand for the integral on the line above. We will calculate I separately. For notational simplicity let $\Lambda = R_c/R$. Using the transformation $R_c/r = \sin u$, the integral I becomes

$$\begin{aligned} I &= \int_{\pi/2n}^{\arcsin(\Lambda)} -R_c u\cos(u)\big(\sin(u)\big)^{-2}\, du = \int_{\pi/2n}^{\arcsin(\Lambda)} R_c u\, d\Big(\big(\sin(u)\big)^{-1}\Big) \\ &= R_c\, u\big(\sin(u)\big)^{-1}\Big|_{\pi/2n}^{\arcsin(\Lambda)} - \int_{\pi/2n}^{\arcsin(\Lambda)} R_c\big(\sin(u)\big)^{-1} du \\ &= R_c\, u\big(\sin(u)\big)^{-1}\Big|_{\pi/2n}^{\arcsin(\Lambda)} - R_c\log\big|\tan(u/2)\big|\Big|_{\pi/2n}^{\arcsin(\Lambda)} \\ &= R_c\arcsin(\Lambda)\Lambda^{-1} - R_c(\pi/2n)\big(\sin(\pi/2n)\big)^{-1} \\ &\quad - R_c\log\big|\tan\big(\arcsin(\Lambda)/2\big)\big| + R_c\log\big|\tan(\pi/4n)\big|. \end{aligned}$$

Substituting the value of I into (1) and collecting terms together we have that

$$\begin{aligned} &P\big(r > r_0, \phi > \arcsin(R_c/r)\big) \\ &\quad = 1 - \frac{2n}{\pi}\arcsin(\Lambda) + \frac{2n}{\pi}\Lambda\log\big|\tan\big(\arcsin(\Lambda)/2\big)\big| - \frac{2n}{\pi}\Lambda\log\big|\tan(\pi/4n)\big| \\ &\quad = 1 - \frac{2n}{\pi}\left(\arcsin(\Lambda) + \Lambda\log\left|\frac{\tan(\pi/4n)}{\tan(\arcsin(\Lambda)/2)}\right|\right). \end{aligned}$$

Thus the probability, p, that one of the radial cuts hits the coin is

$$p = \frac{2n}{\pi}\left(\arcsin(\Lambda) + \Lambda\log\left|\frac{\tan(\pi/4n)}{\tan(\arcsin(\Lambda)/2)}\right|\right). \tag{2}$$

Numerical application Using expression (2) from above, we can examine p for specific values of R^* and R_c, and for various values of n. For instance assume that we

have the realistic scenario that the radius of the coin is $R_c = 1$ cm and that of the cake is $R^* = 16$ cm. TABLE 1 gives the value of p for selected values of n. Surprisingly enough, we observe that even when n is equal to 2, which means that the cake is cut into four equal parts, the probability that the knife hits the coin is very high (close to 30%). As expected, p is increasing as n increases and for $n = 23$, p is just below 1. For $n \geq 24$, the probability of an intersection is clearly 1 since for those values it holds true that $R \sin(\pi/2n) \leq R_c$.

TABLE 1: Probability of intersection for selected values of n.

n	2	4	8	12	16	20	22	23
p	0.2987	0.4730	0.7073	0.8535	0.9422	0.9881	0.9978	0.9997

Remark In this note, we consider only the case where the coin is dropped at random on a circle in the plane. However, various extensions of that problem can be formulated. For example, in $\mathbb{R}^3$ one might consider the situation where the coin takes any position in an object like a cylinder, or a sphere, not necessarily in a uniform manner.

Acknowledgment. I would like to thank the referees for their valuable suggestions and comments which lead to an improved version of the manuscript. I would also like to thank Professor Tasos Christofides for suggesting the problem and for his guidance during the preparation of the manuscript.

REFERENCES

1. Solomon, Herbert, *Geometric Probability*, CBMS **28**, Society for Industrial and Applied Mathematics, Philadelphia, 1978.
2. Uspenski, J.V., *Introduction to Mathematical Probability*, McGraw-Hill, New York, 1937.

Replacement Costs: the Inefficiencies of Sampling with Replacement

EMILY S. MURPHREE
Miami University
Oxford, Ohio 45056
murphres@muohio.edu

When we deal five cards in poker, we do not deal the same card twice. The cards dealt are all distinct (unless the deck is rigged). This is typical of most sampling problems, where samples are chosen *without replacement*. This means that once chosen, an object is not eligible to be selected again.

However, there are interesting practical problems involving sampling *with replacement*. For example, one might need to evaluate the performance of a computer program intended to generate 5-digit random numbers. If the numbers are truly random, then each digit is equally likely to be any of the values 0–9 and the digits are independent of one another. Thus if the program is working properly, we can consider each 5-digit number to be a sample of size five chosen with replacement from the popula-

tion $\{0, 1, \ldots, 9\}$. To evaluate the program, we would compare the properties of the samples it generates to the properties we expect given randomness.

We will study the number of distinct items appearing in a sample of size r chosen with replacement from a population of size N. The random variable $X(N, r)$ will denote this number. Depending on the luck of the draw, this number could be as small as 1, if we happened to choose the same item over and over again. It cannot be larger than either our sample size r or our population size N.

If we knew the probabilities of $X(N, r)$ assuming its possible values, we could evaluate how well the computer program does to generate numbers randomly. We could also use information about $X(N, r)$ to compare samples chosen with and without replacement. Statisticians generally choose samples without replacement because they are trying to infer the properties of the population. By choosing without replacement, they get a peek at r distinct items and tend to get a fuller picture of the population than they do when sampling with replacement. By comparing the expected size of $X(N, r)$ to r, we can judge the inefficiencies of sampling with replacement.

Unfortunately, deriving the probability distribution of $X(N, r)$ is frustratingly difficult. Counting arguments are hopeless if N and r are even moderate in size. For example, if a pond contains $N = 15$ bass and we catch and release $r = 10$ bass, tagging all untagged fish as we go, we might want to know the chance of tagging 5 total bass. A counting argument would require us to enumerate the number of ways of catching just 5 different fish. The list would have to include situations where we caught each of 5 fish twice; where 3 fish are caught twice, 1 is caught three times, and 1 once; where 1 fish is caught six times and 4 are caught once each; and so forth. This approach is not fruitful.

Nevertheless, the probability distribution, mean, variance, and factorial moments of $X(N, r)$ are known and can be found, for example, in Stevens [7] and in Craig [2]. Unfortunately, these results rely on the so-called "leading differences" of powers of the natural numbers. Current undergraduates are likely to be befuddled by the derivations in these papers because they depend on fairly sophisticated knowledge of the calculus of finite differences.

Questions about numbers of distinct items fall under the umbrella of the "occupancy problem" in probability because $X(N, r)$ also represents the number of urns that are occupied by at least one ball when r balls are randomly distributed among N urns. Hoel, Port, and Stone's *Introduction to Probability Theory* [4] derives the distribution of $X(N, r)$ by using the inclusion-exclusion principle and the probability that k specified urns are empty. Their occupancy section is starred as an optional topic, and most modern mathematical statistics texts omit the problem altogether. Authors probably believe that the mathematical machinery required is too daunting for the payoff gained.

However, the problem can be tackled using a fresh approach—avoiding methods that many students find mysterious. By regarding the sampling experiment as a Markov chain problem, we can derive the probability distribution of $X(N, r)$ by standard methods from linear algebra. Next, we find the mean and variance of $X(N, r)$ by very simple arguments involving Bernoulli random variables. Finally, we use the results to test a random number generator using a chi-squared goodness-of-fit test.

The distribution of the number of distinct items Notice that in choosing r times with replacement from a population of size N, we are performing an r-stage experiment. Let us say that that our experiment is in *state* k at *time* t if we have observed k distinct items after having sampled t times. In order to describe the possible outcomes at time $t + 1$, we only need to know the state at time t; we can ignore what happened at

earlier times. This scenario is the hallmark of an experiment suited for analysis using Markov chains. By describing the states of the experiment (or chain) and the probabilities of moving from one state to another, we can unravel the sampling problem step-by-step.

In our chain, the states are $\{0, 1, \ldots, N\}$. The system will necessarily be in state 1 at time 1. If we are in state k at time t, then only two transitions are possible: we will either remain in k at time $t+1$ with probability $p_{k,k} = k/N$ or we will move to state $k+1$ with probability $p_{k,k+1} = (N-k)/N$. (In more general Markov chains, state-to-state movement is less restricted than this and movement can occur between nonadjacent states and from *higher* to *lower* states.) These one-step transition probabilities depend only on the current state; they do not depend on how we arrived at that state or even the number of steps we took to get there. We can therefore treat the sampling problem as a time-homogeneous Markov chain. (See, for example, Feller [**3**, Chapter 15] for an elaboration.)*

The properties of $X(N, r)$ can be derived from what is called the *transition matrix*:

$$P_{N\times N} = \begin{bmatrix} \frac{1}{N} & \frac{N-1}{N} & 0 & 0 & 0 & \ldots & 0 \\ 0 & \frac{2}{N} & \frac{N-2}{N} & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \ldots & \frac{k}{N} & \frac{N-k}{N} & \ldots & 0 \\ \vdots & \vdots & & & & & 0 \\ 0 & 0 & \ldots & 0 & 0 & \frac{N-1}{N} & \frac{1}{N} \\ 0 & 0 & \ldots & & & 0 & 1 \end{bmatrix}.$$

The (i, j) element of P is the probability of moving from state i to state j in one step. Similarly, the (i, j) element of P^m is the probability of moving from state i to state j in m steps.

We are concerned with $X(N, r)$, the state of the chain at time r. This is just the state of the chain $r-1$ steps after having entered state 1. Hence the probability that $X(N, r) = k$ is $p_{1k}^{(r-1)}$, the probability of moving from state 1 to state k in $r-1$ steps. This is the entry in row 1 and column k of the matrix P^{r-1}.

Ordinarily, deriving formulas for powers of matrices is tedious if not impossible. Fortunately, P is a simple matrix, which is easily expressed as $P = S\Lambda S^{-1}$, where S is a matrix whose columns are eigenvectors of P and Λ is a diagonal matrix whose entries are the corresponding eigenvalues. As is known from linear algebra [**6**, p. 299], this diagonalization is possible whenever a matrix has a full set of linearly independent eigenvectors. Fortunately, P does. Once P is written in this fashion, P^{r-1} is just $S\Lambda^{r-1}S^{-1}$ and hence the probability distribution of $X(N, r)$ is found in the first row of this matrix.

It is not difficult to find that $1/N,\ 2/N, \ldots, k/N, \ldots, 1$ are the eigenvalues of P and that an eigenvector corresponding to the eigenvalue k/N is

$$\left(\binom{N-1}{k-1} \quad \binom{N-2}{k-2} \quad \ldots \quad \binom{N-k}{0} \quad 0 \quad 0 \quad \ldots \quad 0\right)^T.$$

*Editor's note: Readers can see another application of Markov chains in the Note by Kiser, McCready, and Schwertman in this issue.

Thus

$$S = \begin{bmatrix} 1 & N-1 & \binom{N-1}{2} & \cdots & \binom{N-1}{k-1} & \cdots & 1 \\ 0 & 1 & \binom{N-2}{1} & \cdots & \binom{N-2}{k-2} & \cdots & 1 \\ \vdots & \vdots & & \cdots & & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \binom{N-k}{0} & \cdots & 1 \\ \vdots & \vdots & & & & \cdots & 1 \\ 0 & 0 & & & 0 & & 1 \\ 0 & 0 & 0 & & & 0 & 1 \end{bmatrix}.$$

S^{-1} has the same entries as S itself except for the presence of alternating plus and minus signs. In particular, the (i, j) entry in S^{-1} is $s_{ij}(-1)^{i+j}$.

Thus

$$P^{r-1} = [S\Lambda^{r-1}]S^{-1}$$

$$= \begin{bmatrix} \left(\frac{1}{N}\right)^{r-1} & (N-1)\left(\frac{2}{N}\right)^{r-1} & \binom{N-1}{2}\left(\frac{3}{N}\right)^{r-1} & \cdots & \binom{N-1}{N-2}\left(\frac{N-1}{N}\right)^{r-1} & 1 \\ 0 & \left(\frac{2}{N}\right)^{r-1} & \binom{N-2}{1}\left(\frac{3}{N}\right)^{r-1} & \cdots & \binom{N-2}{N-3}\left(\frac{N-1}{N}\right)^{r-1} & 1 \\ 0 & 0 & \left(\frac{3}{N}\right)^{r-1} & \cdots & \binom{N-3}{N-4}\left(\frac{N-1}{N}\right)^{r-1} & 1 \\ \vdots & \vdots & & & & 1 \\ 0 & 0 & 0 & & & 1 \\ 0 & 0 & 0 & \cdots\ 0 & \left(\frac{N-1}{N}\right)^{r-1} & 1 \\ 0 & 0 & 0 & \cdots\ 0 & 0 & 1 \end{bmatrix}$$

$$\times \begin{bmatrix} 1 & -(N-1) & \binom{N-1}{2} & \cdots & (-1)^{k+1}\binom{N-1}{k-1} & \cdots & (-1)^{N+1} \\ 0 & 1 & -\binom{N-2}{1} & \cdots & (-1)^{k+2}\binom{N-2}{k-2} & \cdots & (-1)^{N+2} \\ \vdots & \vdots & & \cdots & & \cdots & 1 \\ 0 & 0 & 0 & \cdots & (-1)^{2k}\binom{N-k}{0} & \cdots & (-1)^{N+k} \\ \vdots & \vdots & & & & \cdots & \vdots \\ & 0 & & & 0 & & (-1)^{2N-1} \\ 0 & 0 & 0 & & & 0 & 1 \end{bmatrix}$$

Hence $P\{X(N, r) = k\} = p_{1k}^{(r-1)}$ is the result of multiplying the first row of $S\Lambda^{r-1}$ into the kth column of S^{-1} and is thus

$$\sum_{j=1}^{k}\left(\frac{j}{N}\right)^{r-1}\binom{N-1}{j-1}\binom{N-j}{k-j}(-1)^{k+j} = \binom{N-1}{k-1}\sum_{j=1}^{k}\left(\frac{j}{N}\right)^{r-1}\binom{k-1}{j-1}(-1)^{k+j}. \tag{1}$$

This formula agrees with the result (3.11) of Stevens [7], but it has the advantage of not being expressed in terms of "differences of zero."

The mean and variance of the distribution It is difficult to use (1) to find expected values associated with the number of distinct items. Stevens finds the moments of $X(N, r)$ from the "factorial moment generating function" of $X(N, r)$. (The factorial moment generating function of a random variable Y is $E[t^Y]$.) An easier approach, at least for finding the mean and variance, is to express $X(N, r)$ in terms of N Bernoulli

random variables and to use some simple facts about the moments of Bernoulli random variables.

The key observation is that N is the sum of two random terms: the number of items that were sampled at least once plus the number of items that were never chosen. That is, $N = X(N, r) + Y$, where Y is the number of items never chosen. Rather than tackle $X(N, r)$ head-on, we deduce its properties from those of Y.

We can write $Y = \sum_{i=1}^{N} B_i$ where B_i is a Bernoulli (or indicator) random variable that is 1 only if the ith item in the population is never sampled. Then $p = P\{B_i = 1\} = ((N-1)/N)^r$.

It follows immediately that

$$E\big[X(N,r)\big] = E[N - Y] = N - \sum_{i=1}^{N} E[B_i] = N - Np$$

$$= N\left[1 - \left(\frac{N-1}{N}\right)^r\right]. \tag{2}$$

This matches Stevens's result (3.41) and shows the expectation approaches N exponentially as r approaches infinity. For finite r, this formula implies that if we choose N items with replacement out of N, we should expect just

$$N\left[1 - \left(\frac{N-1}{N}\right)^N\right] \approx N\left[1 - e^{-1}\right]$$

of them to be different. Sampling without replacement would guarantee our selecting all N, so the "cost" of replacement is that we expect only about 63% efficiency.

Since $X(N, r) = N - Y$, its variance is equal to the variance of Y. If Y were the sum of *independent* indicator variables $B_1, B_2, \ldots, B_N$, its variance would be the sum of the variances of these Bs. However, the Bs are not independent. If the ith object is never sampled, it is more likely that the jth object is sampled. That is, if $B_i = 1$, it is more likely than usual for $B_j = 0$. B_i and B_j are negatively associated and therefore their covariance $\mathrm{Cov}[B_i, B_j] = E[\{B_i - E(B_i)\}\{B_j - E(B_j)\}]$ is negative. Thus

$$\mathrm{Var}\left[\sum_{i=1}^{N} B_i\right] = \sum_{i=1}^{N} \mathrm{Var}(B_i) + \sum_{i \neq j} \mathrm{Cov}(B_i, B_j).$$

(See, for example, Wackerly [**8**, pp. 255–257] for details in computing variances of sums.)

Given the simple structure of Bernoulli random variables, we know that

$$\mathrm{Var}(B_i) = p(1-p) = \left(\frac{N-1}{N}\right)^r \left[1 - \left(\frac{N-1}{N}\right)^r\right]$$

for each i. For $i \neq j$, $\mathrm{Cov}(B_i, B_j) = E[B_i B_j] - p^2$, where

$$E[B_i B_j] = P\{\text{neither the } i\text{th nor the } j\text{th item is sampled}\} = \left(\frac{N-2}{N}\right)^r.$$

Thus

$$\mathrm{Cov}(B_i, B_j) = \left[\left(\frac{N-2}{N}\right)^r - \left(\frac{N-1}{N}\right)^{2r}\right] < 0 \quad \text{and}$$

$$\begin{aligned}\operatorname{Var}\left[X(N,r)\right] &= N\left(\frac{N-1}{N}\right)^r\left[1-\left(\frac{N-1}{N}\right)^r\right] \\ &\quad + N(N-1)\left[\left(\frac{N-2}{N}\right)^r-\left(\frac{N-1}{N}\right)^{2r}\right] \\ &= \frac{(N-1)^r}{N^{r-1}}+\frac{(N-1)\,(N-2)^r}{N^{r-1}}-\frac{(N-1)^{2r}}{N^{2r-2}}. \qquad (3)\end{aligned}$$

Again, this is equivalent to Stevens' formula. It is interesting to note that if $r = N$,

$$\operatorname{Var}[X(N,N)] = \frac{(N-1)^N}{N^{N-1}}+\frac{(N-1)\,(N-2)^N}{N^{N-1}}-\frac{(N-1)^{2N}}{N^{2N-2}} \approx N\left(e^{-1}-e^{-2}\right).$$

Of course, as r approaches infinity, $\operatorname{Var}[X(N,r)]$ approaches zero, because with sufficient sampling one will finally choose every single item.

Testing for randomness Suppose we want to check on the randomness of 350 5-digit numbers generated by MINITAB (version 13), a software package used in many undergraduate statistics courses. One test used is the so-called *poker test*, which is based on noting how often the 5 digits contain either no matches, one pair, two pairs, three of a kind, a full house, four of a kind, or five of a kind. A chi-squared goodness-of-fit test can be used to decide whether the frequencies of these seven categories are consistent with the hypothesis of randomness.

A variation on this test is to ask how many distinct digits appear in the 5-digit sequences. This is a question about $X(10, 5)$. When there are no matches, $X(10, 5) = 5$; it is 4 when there is exactly one pair; 3 when there are two pairs or three of a kind; 2 when there is a full house or four of a kind; and 1 if there are 5 of a kind.

If the program is working properly, formula (1) tells us that

$$P\{X(10,5)=k\} = \binom{9}{k-1}\sum_{j=1}^{k}\left(\frac{j}{10}\right)^4\binom{k-1}{j-1}(-1)^{k+j}.$$

Evaluating, we find $X = X(10, 5)$ has probability distribution

X	**1**	**2**	**3**	**4**	**5**
$P\{X=x\}$	$1/10^4$	$135/10^4$	$1800/10^4$	$5040/10^4$	$3024/10^4$

One can easily see that this distribution has mean $4.0951 = 10[1-(9/10)^5]$ and variance $.52825599 = 9^5/10^4 + 9(8^5)/10^4 - 9^{10}/10^8$, in agreement with (2) and (3).

Thus, to check our 350 5-digit numbers, we can use a chi-squared test to compare the observed frequency O_i of the event $\{X = i\}$ with its expected frequency E_i under the hypothesis of randomness. (The expected frequency of category i is $E_i = 350\ P\{X(10, 5) = i\}$.) The observed and expected counts are:

X	**1**	**2**	**3**	**4**	**5**
O_i	0	7	58	183	102
E_i	.035	4.725	63	176.4	105.84

If the terms $[0_i - E_i]^2/E_i$ are small, the test confirms that the observed and expected values are close enough to suggest randomness. Dividing by E_i accounts for the fact that a difference of 8, for example, is much more alarming when our expected count

is 5 than when it is 200. Because the test requires certain minimum expected cell frequencies, we begin by combining the first two categories. This forces all the E_is to be at least 1 and makes 75% of them 5 or more, thereby ensuring the chi-squared test is appropriate. The resulting test statistic is

$$\chi^2 = \sum_{i=1}^{4} [0_i - E_i]^2/E_i = (7 - 4.76)^2/4.76 + (58 - 63)^2/63$$
$$+ (183 - 176.4)^2/176.4 + (102 - 105.84)^2/105.84 = 1.837.$$

If the 5-digit numbers have been generated at random, the test statistic is the value of an approximate chi-squared random variable having expected value 3. Values significantly greater than 3 indicate systematic departures from randomness. Our value of 1.837 shows a better than expected agreement. (A statistician would not consider rejecting the hypothesis of randomness unless the test statistic exceeded 6.25, the critical value for a level .10 test.) Thus the MINITAB data pass our test with flying colors.

(Notes on this test: (a) The degrees of freedom are one fewer than the number of categories, which in our case is $4 - 1$. (b) Not all authors agree on how large a sample is required for the chi-squared test to be appropriate. There is general agreement that all E_is should be at least one. Cochran [**1**] suggests that at least 80% of the expected cell frequencies should be 5 or greater. Moore [**5**] says this is too conservative.)

REFERENCES

1. W. G. Cochran, Some methods of strengthening the common χ^2 tests, *Biometrics* **10**, 417–451.
2. C. C. Craig, On utilization of marked specimens in estimating the population of flying insects, *Biometrika* **40** (1953), 170–176.
3. William Feller, *An Introduction to Probability Theory*, Vol. 1, John Wiley & Sons, New York, 1968, 372–384.
4. Paul G. Hoel, Sidney C. Port, and Charles J. Stone, *Introduction to Probability Theory*, Houghton Mifflin, Boston, 1971, 43–45.
5. David S. Moore, Tests of chi-squared type. In Ch. 3, R. B. D'Agostino and M. A. Stephens, *Goodness-of-Fit Techniques*, Marcell Dekker, New York, 1986.
6. David Poole, *Linear Algebra*, Brooks/Cole, Pacific Grove, CA, 2003.
7. W. L. Stevens, Significance of grouping, *Annals of Eugenics* **8** (1937), 57–69.
8. Dennis D. Wackerly, William Mendenhall III, and Richard L. Scheaffer, *Mathematical Statistics with Applications*, Duxbury, Pacific Grove, CA, 2002.

Can the Committee Meet? A Markov Chain Analysis

TERRY L. KISER
THOMAS A. McCREADY
NEIL C. SCHWERTMAN
California State University, Chico
Chico, CA 95929

Most faculty members have faced the challenge of trying to schedule a committee meeting at a time when all members could attend. And most faculty members have an intuitive sense of the probability that they will be successful. For example, the authors teach in a department where the typical course load is four courses, scheduled into 15 available weekly time blocks. Prior to writing this note, our perception was that for committees consisting of more than five members, finding an open slot would

be unlikely. The abundance of 7:00 A.M. and 5:00 P.M. committee meetings on our campus seems to bear this out!

Scheduling a committee meeting presents a relevant and interesting, yet simple, application of Markov chains. As we show, this can be thought of as an unusual blend of two types of *occupancy problems*. After solving the general problem, we summarize our findings, both graphically and analytically, for several settings, including that of our own campus. How does your institution compare with these?

We will refer to the set of possible nonoverlapping meeting times for classes (for example, MWF 1–2) as time slots. To model the arranging of a meeting assume there are N such time slots, typically called *cells* in the occupancy literature, into which classes are assigned. Furthermore, assume that, for each teacher, a course load of n courses is randomly assigned to n different time slots. If we were considering the schedule of a single teacher, this would be a single occupancy problem, since most of us cannot teach two classes at the same time. However, with a committee of more than one member, it is possible and even likely that the courses will overlap. Thus, we need a second type of occupancy model that allows multiple occupancies of the various time slots or cells. For more on occupancy problems see, for instance, Feller [**1**, pp. 38–47], or Parzen [**3**, pp. 69–76].

In practice, other factors, such as office hours, personal preferences, and other commitments complicate the process of finding an available time. Let us assume, however, that all these other types of conflicts can be ignored and that only the course load time slots limit the availability of the member. We will construct what is called a *Markov chain* to represent this model. This Markov chain will enable us to compute the probabilities that, with a committee of k members, there is some time slot available. We will also be able to compute the probability that any specific numbers of time slots is available.

The Markov chain A *Markov process* involves transitions between conditions known as *states,* with the criterion that probabilities governing the next state depend only on the current state. At first, this sounds nothing like our scheduling problem.

Our strategy is to begin with a committee with no members and proceed to add one member at a time to the schedule, while keeping track of occupied slots. The *present state* of this process is the number of *occupied slots*, that is, the periods in which committee members are currently assigned classes, assuming that each of k members has n courses on the schedule. We will move to the next state by adding another committee member.

Since the probabilities of various outcomes at the next state depend only on the present state, this fits the criteria of a Markov process. More precisely, the conditional probability of a transition from the present state to the next state does not depend on how the present stage was achieved. That is, it is only necessary to know that i time slots were already occupied by the classes of the current k members of the committee in order to determine the probabilities that $i, i+1, \ldots, \min(i+n, N)$ different time slots are occupied after another committee member is added. (Recall that N is the total number of time slots.)

Knowing that our situation is a Markov process, we can use a Markov chain to determine the probabilities of the number of slots occupied by the members of committees of various sizes. The *Markov chain* consists of a transition matrix T and an initial vector V_0, as we will describe below.

For a more detailed discussion of Markov processes and Markov chains see, for example, Karlin and Taylor [**2**, pp. 45–47], Feller [**1**, pp. 419–421], or Parzen [**3**, pp. 136–140].*

*Editor's note: Readers can see another application of Markov chains in the Note by Murphree in this issue.

The transition matrix The heart of our analysis is a square matrix, T, called the *transition matrix*. It holds the probabilities of moving between states when one more committee member is added. More specifically, define $T(i, j)$ to be the probability of moving from state i, where i cells (time slots) are occupied, to state j. Since the possible values of i are $i = 0, n, n+1, \ldots, N$, $T(i, j)$ is not the element of the ith row, jth column of T, unless $i = j = 0$. Note that T is an $N - n + 2$ by $N - n + 2$ square matrix.

As before, let n be the number of classes taught by each committee member and let N be the total number of time slots available during the week in which classes can be scheduled. Note that i, the number of occupied time slots, jumps from zero to n with the addition of the first committee member. This means that, $T(0, n) = 1$.

Since adding a committee member never reduces the number of slots occupied, $j < i$ means $T(i, j) = 0$.

For $n \le i \le j \le N$, we compute $T(i, j)$ by simple counting arguments. There are $\binom{N}{n}$ ways to pick the n slots at random for the new member. In order to have j slots occupied after this addition, this person must have $j - i$ classes that meet in the previously unused time slots (in $\binom{N-i}{j-i}$ ways) and $n - (j - i)$ classes that meet during the i time slots already occupied by previous members (in $\binom{i}{n-j+i}$ ways). Assembling these ideas gives the transition matrix:

$$T(i, j) = \begin{pmatrix} \binom{N-i}{j-i}\binom{i}{n-j+i}/\binom{N}{n}, & n \le i \le j \le N \\ 1 & i = 0,\ j = n \\ 0 & \text{otherwise} \end{pmatrix}$$

Readers may recognize the entries as hypergeometric probabilities.

Calculating the probability distribution Our Markov chain begins with an empty committee, which certainly occupies no time slots. The probability that no slots are occupied is 1, while the probability that any other number of slots is occupied is 0. We record this as the initial vector,

$$V_0 = \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix}.$$

For a committee of k members, we define V_k to be the $(N - n + 2)$-dimensional row vector containing the probabilities that the various possible numbers of time slots are occupied. More precisely, for let $V_k(m)$ denote the mth component of V_k. If $m = 1$, $V_k(1)$ is the probability that no cells are occupied. For $m > 1$, $V_k(m)$ is the probability that exactly $m + n - 2$ time slots are occupied.

It turns out **[1, 3]** that the transition matrix T is exactly what is needed to transform the vector V_{k-1} to V_k. In particular, the distribution of the probabilities with the addition of the first person is $V_1 = V_0 \cdot T$, which is simply

$$V_1 = \begin{bmatrix} 0 & 1 & \cdots & 0 \end{bmatrix}.$$

This matches with intuition, since we know that exactly n slots must be occupied.

In general, to compute the probabilities of various levels of occupancy after the kth person has been added, we use the formula

$$V_k = V_{k-1} \cdot T = (V_{k-2} \cdot T) \cdot T = V_{k-2} \cdot T^2 = \cdots = V_0 \cdot T^k.$$

Examples Our university is typical of many teaching universities. The standard teaching assignment is 4 three-unit courses per week and there are 15 available time slots in a week to accommodate the classes; that is, $N = 15$ and $n = 4$.

The transition matrix T is given by $\frac{1}{1365}T'$, where $T' =$

Present states (i) \ Future states (j)	0	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1365	0	0	0	0	0	0	0	0	0	0	0
4	0	1	44	330	660	330	0	0	0	0	0	0	0
5	0	0	5	100	450	600	210	0	0	0	0	0	0
6	0	0	0	15	180	540	504	126	0	0	0	0	0
7	0	0	0	0	35	280	588	392	70	0	0	0	0
8	0	0	0	0	0	70	392	588	280	35	0	0	0
9	0	0	0	0	0	0	126	504	540	180	15	0	0
10	0	0	0	0	0	0	0	210	600	450	100	5	0
11	0	0	0	0	0	0	0	0	330	660	330	44	1
12	0	0	0	0	0	0	0	0	0	495	660	198	12
13	0	0	0	0	0	0	0	0	0	0	715	572	78
14	0	0	0	0	0	0	0	0	0	0	0	1001	364
15	0	0	0	0	0	0	0	0	0	0	0	0	1365

As before, if $m > 1$, the mth element of $V_k = V_0 \cdot T^k$ gives the probability that $m + n - 2$ time slots are occupied when the committee has k members. For our example, the elements of V_5 and V_{10} are the probabilities that $0, 4, 5, 6, \ldots, 15$ time slots are occupied for committees of sizes 5 and 10, respectively. For $k = 5$,

$$V_5 = [0 \quad 2.88 \times 10^{-13} \quad 1.98 \times 10^{-9} \quad 7.82 \times 10^{-7} \quad 6.42 \times 10^{-5} \quad .00174$$
$$.0195 \quad .102 \quad .261 \quad .338 \quad .213 \quad .0597 \quad .00562].$$

For a committee of 10 people,

$$V_{10} = [0 \quad 6.08 \times 10^{-29} \quad 1.31 \times 10^{-21} \quad 1.29 \times 10^{-16} \quad 7.89 \times 10^{-13} \quad 8.03 \times 10^{-10}$$
$$2.19 \times 10^{-7} \quad 2.1 \times 10^{-5} \quad .000823 \quad .0144 \quad .115 \quad .398 \quad .472].$$

As expected, the first elements of V_5 and V_{10}, corresponding to no cells occupied, is zero; a nonempty committee will have at least n slots occupied. For our example with $n = 4$ (four classes per teacher), the mth element of each V_k ($m \geq 2$) is the probability that exactly $m + 2$ slots are occupied.

For example, the tenth and largest element of V_5 is 0.338, which is the probability that exactly 12 time slots of the possible 15 are occupied in a committee with five members. The last element, 0.00562, is the probability that all 15 slots are used; thus, the probability that a committee with five members has at least one time slot available is 0.994.

With these probabilities, it is easy to compute that the expected number of time slots available to a committee of five members is 3.18.

Similarly, for V_{10}, the last element, 0.472, is the largest and represents the probability that all 15 time slots are occupied; thus, 0.528 is the probability that at least one time slot is available to a committee of ten members. The expected number of available time slots for this committee is only 0.675.

Comparing the results, we see that there is almost certain to be at least one time slot available for a meeting with only five committee members, whereas a large committee of ten members has only slightly better than an even chance.

FIGURES 1 and 2 display the probability distribution of the number of the time slots occupied for 15 scheduling periods/week, for various committee sizes and two different teaching loads: $n = 2$ and $n = 4$.

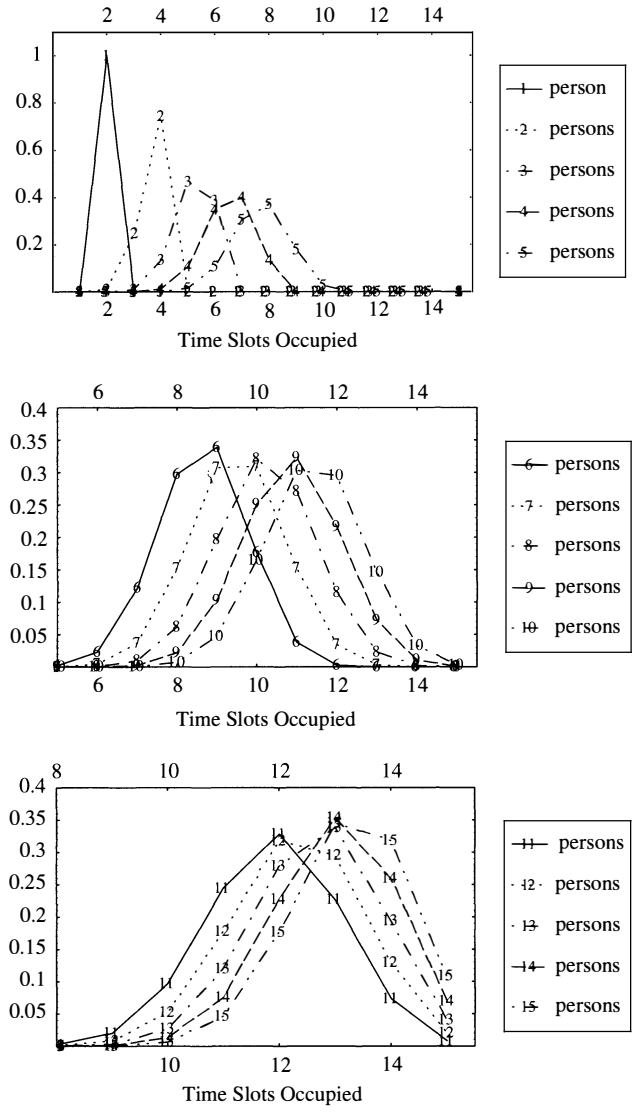


Figure 1 Probabilities of the number of slots occupied with $N = 15$, $n = 2$

The patterns in the figures match intuition. Specifically, as the committee size is increased, the most likely number of occupied time slots also increases, but the associated probabilities decrease. Furthermore, as n, the number of classes taught by each teacher increases, finding a time when all committee members are available becomes less likely. For a teaching assignment of two classes per week ($n = 2$), even a committee of fifteen has a good chance of finding a meeting time. However, to have a good chance of an available time slot (a probability of approximately .8), the maximum committee sizes are 11, 8, and 6 for teachers teaching three, four, and five classes per week ($n = 3, 4, 5$), respectively.

These figures are helpful in understanding the impact of the teaching load and committee size on the chances of finding a meeting time. It may be of interest to know the maximum number of members a committee may have in order to be, say, approximately 90%, 95%, and 99% confident that there will be at least one time slot where

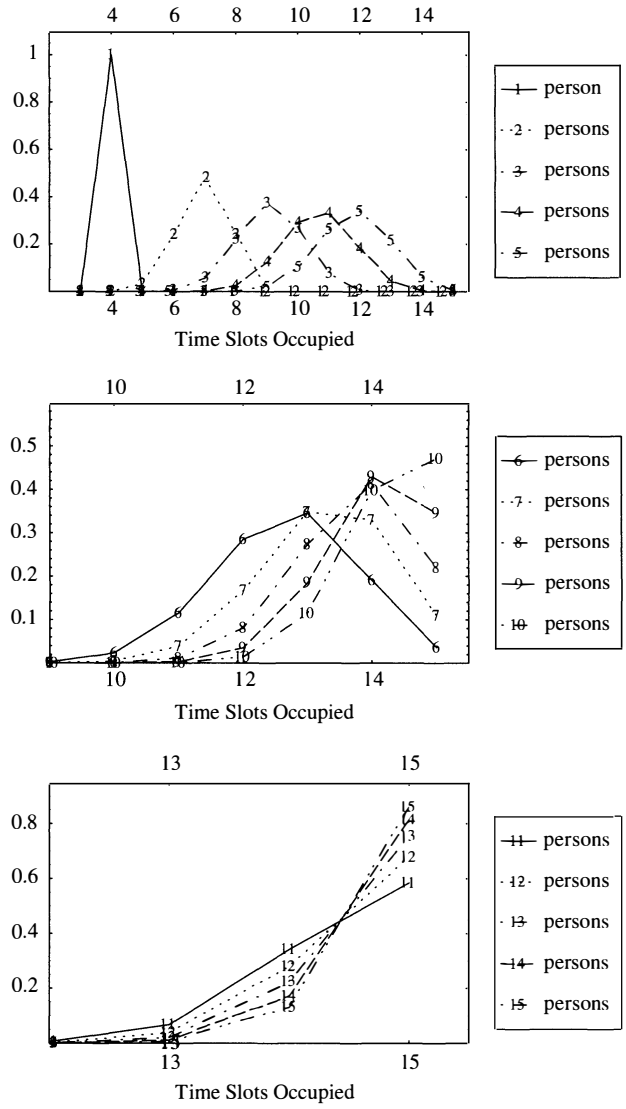


Figure 2 Probabilities of the number of slots occupied with $N = 15$, $n = 4$

all committee members are available. The table below provides these maxima for the usual number of possible time slots for the 8 AM–5 PM workday, that is, $N = 15$, and for teaching assignments of $n = 2, 3, 4, 5$ classes.

TABLE 1: Maximum number of committee members and exact probabilities that at least one time slot is available

n, number of classes/teacher	Approximate confidence level		
	90%	95%	99%
2	15 ($p = .8925$)	13 ($p = .9597$)	11 ($p = .9916$)
3	10 ($p = .8684$)	9 ($p = .9314$)	7 ($p = .9930$)
4	7 ($p = .8900$)	6 ($p = .9631$)	5 ($p = .9944$)
5	5 ($p = .9320$)	5 ($p = .9320$)	4 ($p = .9915$)

While not all of the assumptions of the model will be satisfied in every case, nevertheless, this analysis might be used to justify limiting the size of committees. Now, if we could only come up with an analysis to justify limiting the number of committees we are assigned to!

Acknowledgment. The authors would like to express their appreciation to the reviewers for many helpful suggestions.

REFERENCES

1. W. Feller, *An Introduction to Probability Theory and Its Applications*, Vol. I, John Wiley & Sons Inc., New York, 1968.
2. S. Karlin, and H. M. Taylor, *A First Course in Stochastic Processes*, 2nd ed., Academic Press, New York, 1975.
3. E. Parzen, *Modern Probability Theory and Its Applications*, John Wiley & Sons Inc., New York, 1960.

Dirichlet and Fresnel Integrals via Iterated Integration

PAUL LOYA
Binghamton University
Binghamton, NY 13902-6000
paul@math.binghamton.edu

Many articles [**2, 3, 4, 6**] have been devoted to establishing the values of some important improper integrals:

$$\int_0^\infty \frac{\sin x}{x}\,dx = \frac{\pi}{2} \quad \text{and} \quad \int_0^\infty \frac{\cos x}{\sqrt{x}}\,dx = \int_0^\infty \frac{\sin x}{\sqrt{x}}\,dx = \sqrt{\frac{\pi}{2}}.$$

The first integral is called the Dirichlet integral and the other two are called Fresnel integrals. One way to establish these formulas is to consider the iterated integrals of the functions $f(x, y) = e^{-xy}\sin x$ and $g(x, y) = y^{-1/2}e^{-xy+ix}$, respectively, over $[0, \infty) \times [0, \infty)$. For instance, if only we could justify switching the order of integration, we would evaluate the Dirichlet integral like this:

$$\int_0^\infty \left(\int_0^\infty e^{-xy}\sin x\,dy\right)dx = \int_0^\infty \left(\int_0^\infty e^{-xy}\sin x\,dx\right)dy. \tag{1}$$

Since $\int_0^\infty e^{-xy}\sin x\,dy = \sin x/x$, the left-hand integral is $\int_0^\infty (\sin x)/x\,dx$. In view of the integration formula

$$\int e^{-xy}\sin x\,dx = -\frac{e^{-xy}}{1+y^2}(y\sin x + \cos x) + C, \tag{2}$$

which is proved using integration by parts, the right-hand integral in (1) is

$$\int_0^\infty \frac{1}{1+y^2}\,dy = \lim_{t\to\infty} \tan^{-1}(y)\Big|_{y=0}^{y=t} = \frac{\pi}{2}.$$

Hence, we have computed the value of the Dirichlet integral: $\int_0^\infty (\sin x)/x\,dx = \pi/2$. Unfortunately, justification for these steps is not at all obvious! The reason is that the

standard hypotheses justifying iterating improper integrals, namely Fubini's theorem, which requires absolute integrability, do not apply to the above mentioned f and g. After all, $f(x,0)$ is $\sin(x)$, which is certainly not integrable over the whole line, and $g(x,0)$ is not even defined.

However, in this paper we have just the right theorem to justify the desired steps. This theorem applies to the functions f and g and is useful and appropriate in an undergraduate analysis course for two reasons: (1) The hypotheses are straightforward to verify and they apply to many important examples (see Examples 1–4); (2) The proof is very short (given certain well-known results).

THEOREM. *Let $F(x, y)$ be a continuous function on $(a, \infty) \times (\alpha, \infty)$, where a and α are real numbers, and suppose that the improper integrals*

$$G(x) = \int_{\alpha^+}^{\infty} F(x, y)\, dy \quad \text{and} \quad H(y) = \int_{a^+}^{\infty} F(x, y)\, dx \tag{3}$$

exist and converge uniformly for x and y restricted to compact subintervals of (a, ∞) and (α, ∞), respectively. In addition, suppose that for all $b, c > a$,

$$\left| \int_b^c F(x, y)\, dx \right| \leq M(y), \tag{4}$$

where $\int_{\alpha^+}^{\infty} M(y)\, dy$ exists. Then the improper integrals

$$\int_{a^+}^{\infty} G(x)\, dx \quad \text{and} \quad \int_{\alpha^+}^{\infty} H(y)\, dy \tag{5}$$

exist and are equal.

The integrals in this theorem are Riemann integrals and they are improper at a, α, and ∞; hence the plus signs on a and α. Since the integrals in (3) are uniformly convergent, $G(x)$ and $H(y)$ are continuous on their respective domains [**1**, Th. 33.6], which guarantees they are Riemann integrable over compact subintervals of their respective domains. If all integrals are understood as Kurzweil-Henstock integrals or (improper) Lebesgue integrals, or if more knowledge concerning Riemann integrals is assumed, then the hypotheses can be weakened considerably. We invite those readers familiar with more advanced theories to formulate such generalizations.

Before proving our theorem, we need the following standard results (the reader not interested in the proof can skip to Example 1 below):

LEMMA 1.

(a) *If $f(x, y)$ is continuous on a finite rectangle $[a, b] \times [\alpha, \beta]$, then*

$$\int_\alpha^\beta \left(\int_a^b f(x, y)\, dx \right) dy = \int_a^b \left(\int_\alpha^\beta f(x, y)\, dy \right) dx,$$

and the inner integrals are continuous functions of y and x, respectively.

(b) *If $\{f_n\}$ is a sequence of continuous functions on a finite interval $[a, b]$ that converges uniformly on $[a, b]$ to a limit function f, then f is continuous and*

$$\int_a^b f\, dx = \lim_{n\to\infty} \int_a^b f_n\, dx.$$

(c) DOMINATED CONVERGENCE THEOREM. *Suppose that* $f(x) = \lim f_n(x)$ *for all* $x > a$ *where* f *and* f_n, $n \in \mathbb{N}$, *are continuous on* (a, ∞). *Suppose that* $|f_n(x)| \leq M(x)$ *for* $x > a$ *and* $n \in \mathbb{N}$ *where* $\int_{a^+}^{\infty} M(x)\,dx$ *exists. Then* f *has an integral over* $[a, \infty)$ *and*

$$\int_{a^+}^{\infty} f\,dx = \lim_{n\to\infty} \int_{a^+}^{\infty} f_n\,dx.$$

Statements (a) and (b) are found in most elementary analysis books, see, for instance, Bartle [**1**]. The Dominated Convergence Theorem can be found there as Theorem 33.10 and it follows directly from the usual one on compact intervals, a simple proof of which is given by Lewin [**5**]. (Technically, Bartle's Theorem 33.10 is stated for integrals that are improper only at infinity, but an analogous proof works for integrals improper at both limits of integration.)

Now to the proof of the theorem: Let $a < a_n < b_n$ be sequences with $a_n \to a$ and $b_n \to \infty$, and let $\alpha < \alpha_n < \beta_n$ be sequences with $\alpha_n \to \alpha$ and $\beta_n \to \infty$. Since F is continuous on the rectangle $[a_m, b_m] \times [\alpha_n, \beta_n]$, by (a) of Lemma 1,

$$\int_{\alpha_n}^{\beta_n} \left(\int_{a_m}^{b_m} F(x, y)\,dx \right) dy = \int_{a_m}^{b_m} \left(\int_{\alpha_n}^{\beta_n} F(x, y)\,dy \right) dx,$$

and the inner integrals are continuous functions of y and x, respectively. As $n \to \infty$, the inner integral on the right converges uniformly to $G(x)$, so by (b) of Lemma 1, the limit as $n \to \infty$ of the right-hand integral exists and equals $\int_{a_m}^{b_m} G(x)dx$. Thus, the improper integral of the inner integral on the left exists, and

$$\int_{\alpha^+}^{\infty} \left(\int_{a_m}^{b_m} F(x, y)\,dx \right) dy = \int_{a_m}^{b_m} G(x)\,dx. \tag{6}$$

As $m \to \infty$, the continuous function on (α, ∞) given by the inner integral on the left in (6) converges to the continuous function $H(y)$ and by (4), the inner integral is dominated by a function that has an integral over $[\alpha, \infty)$. Thus, (c) of Lemma 1 implies that as $m \to \infty$ the limit of the left-hand side in (6) exists and equals $\int_{\alpha^+}^{\infty} H(y)dy$. It follows that the improper integral $\int_{a^+}^{\infty} G(x)dx$ exists and equals $\int_{\alpha^+}^{\infty} H(y)\,dy$. This completes the proof.

We now demonstrate how easy it is to use this theorem. Henceforth we drop the plus signs on the lower limits of integration to simplify notation.

EXAMPLE 1. For our first example, consider once again $f(x, y) = e^{-xy} \sin x$ on $[0, \infty) \times [0, \infty)$. One can check that f is not absolutely integrable over $[0, \infty) \times [0, \infty)$, so the usual Fubini's theorem does not imply the existence or equality of the iterated integrals of f over this quadrant. However, we can apply our theorem, as we now show. First, because of the exponentially decaying factor, it follows that $\int_0^{\infty} e^{-xy} \sin x\,dy$ and $\int_0^{\infty} e^{-xy} \sin x\,dx$ are uniformly convergent for x and y restricted to compact subintervals of $(0, \infty)$. Second, using the formula (2), one can verify that for all $b, c > 0$,

$$\left| \int_b^c f(x, y)\,dx \right| \leq \frac{K}{1 + y^2}, \quad \text{for some } K > 0,$$

which has an integral on $[0, \infty)$. Thus, the conditions of the theorem are satisfied, and so the formula (1) at the beginning of this paper is indeed true! We can now proceed exactly as we did before to derive the value of the Dirichlet integral:

$$\int_0^{\infty} \frac{\sin x}{x}\,dx = \frac{\pi}{2}.$$

EXAMPLE 2. Now let $g(x, y) = y^{-1/2}e^{-xy+ix}$ on $[0, \infty) \times [0, \infty)$. As with the previous example, the usual Fubini's theorem does not apply to this function, but we shall see that our theorem does apply. Because of the exponentially decaying factor, it follows that $\int_0^\infty y^{-1/2}e^{-xy+ix}\,dy$ and $\int_0^\infty y^{-1/2}e^{-xy+ix}\,dx$ are uniformly convergent for x and y restricted to compact subintervals of $(0, \infty)$. Moreover, one can easily check that for any $b, c > 0$,

$$\begin{aligned}\left|\int_b^c y^{-1/2}e^{-xy+ix}\,dx\right| &= \frac{y^{-1/2}}{|-y+i|}|e^{-cy+ic} - e^{-by+ib}| \\ &\le \frac{1}{\sqrt{y}\sqrt{1+y^2}}(e^{-cy} + e^{-by}) \\ &\le \frac{2}{\sqrt{y}\sqrt{1+y^2}},\end{aligned}$$

which has an integral over $[0, \infty)$. Thus, the conditions of the theorem are met, and so

$$\int_0^\infty \left(\int_0^\infty y^{-1/2}e^{-xy+ix}\,dy\right)dx = \int_0^\infty \left(\int_0^\infty y^{-1/2}e^{-xy+ix}\,dx\right)dy.$$

Since $\int_0^\infty y^{-1/2}e^{-xy+ix}\,dy = e^{ix}\int_0^\infty y^{-1/2}e^{-xy}\,dy = \sqrt{\pi}\,x^{-1/2}e^{ix}$, where we made the change of variables $y \mapsto x^{-1}y^2$ and used the Gaussian integral $\int_0^\infty e^{-y^2}\,dy = \sqrt{\pi}/2$, the left-hand integral is

$$\int_0^\infty \sqrt{\pi}\,x^{-1/2}e^{ix}\,dx = \sqrt{\pi}\int_0^\infty x^{-1/2}\cos x\,dx + i\sqrt{\pi}\int_0^\infty x^{-1/2}\sin x\,dx;$$

on the other hand, changing variables $y \mapsto y^2$, the right-hand integral is

$$\int_0^\infty y^{-1/2}\frac{-1}{-y+i}\,dy = \int_0^\infty \frac{2}{y^2-i}\,dy = \int_0^\infty \frac{2y^2}{1+y^4}\,dy + i\int_0^\infty \frac{2}{1+y^4}\,dy.$$

Each integral on the right has the value $\pi/\sqrt{2}$, which can be found using the method of partial fractions as in [**4**]. Thus, we have computed the Fresnel integrals:

$$\int_0^\infty \frac{\cos x}{\sqrt{x}}\,dx = \int_0^\infty \frac{\sin x}{\sqrt{x}}\,dx = \sqrt{\frac{\pi}{2}}.$$

EXAMPLE 3. Let $0 < a < 1$. Then, arguing as in Example 2, we can apply our theorem to the function $y^{-a}\,e^{-xy+ix}$ on $[0, \infty) \times [0, \infty)$. Working out the iterated integrals in the same spirit as we did in Example 2 and using some elementary properties of the Gamma and Beta functions, we arrive at the following "generalized" Fresnel integrals:

$$\int_0^\infty x^{a-1}\cos x\,dx = \Gamma(a)\cos\left(\frac{a\pi}{2}\right) \quad \text{and} \quad \int_0^\infty x^{a-1}\sin x\,dx = \Gamma(a)\sin\left(\frac{a\pi}{2}\right),$$

where $\Gamma(a)$ is the Gamma function evaluated at a.

EXAMPLE 4. We remark that our theorem immediately implies the celebrated "Weierstrass M-Test" for iterated integrals [**1**, Th. 33.13]: Let $F(x, y)$ be a continuous function on $(a, \infty) \times (\alpha, \infty)$ and suppose that

$$|F(x, y)| \le L(x) \cdot M(y),$$

where $L(x)$ and $M(y)$ have improper integrals over $[a, \infty)$ and $[\alpha, \infty)$, respectively. Then the iterated integrals in (5) exist and are equal.

Finally, we end with a brief outline of how the Dirichlet and Fresnel integrals can be derived from the standard Fubini's theorem. As we already mentioned, both $f(x, y) = e^{-xy} \sin x$ and $g(x, y) = y^{-1/2} e^{-xy+ix}$ are not absolutely integrable on $[0, \infty) \times [0, \infty)$, so, without using the theorem, some ingenious trick is usually required to justify the iteration of integrals. For instance, Bartle [**1**] integrates the function $f(x, y)$ over $[s, \infty) \times [t, \infty)$ with $s, t > 0$, where Fubini's theorem is valid, and after integration is performed, one takes the limits as $s, t \to 0$ to establish Dirichlet's integral. Leonard [**4**] applies Fubini's theorem to $e^{-tx} g(x, y)$ with $t > 0$, which is absolutely integrable on $[0, \infty) \times [0, \infty)$, and, after integrating, takes the limit as $t \to 0$ to establish the Fresnel integrals.

Acknowledgment. The author thanks the referees for helpful comments. The author was supported in part by a Ford Foundation Fellowship.

REFERENCES

1. Robert G. Bartle, *The elements of real analysis*, second ed., John Wiley & Sons, New York-London-Sydney, 1976.
2. Harley Flanders, On the Fresnel integrals, *Amer. Math. Monthly* **89**:4 (1982), 264–266.
3. Waclaw Kozakiewicz, A simple evaluation of an improper integral, *Amer. Math. Monthly* **58**:3 (1951), 181–182.
4. I. E. Leonard, More on Fresnel integrals, *Amer. Math. Monthly* **95**:5 (1988), 431–433.
5. Jonathan W. Lewin, A truly elementary approach to the bounded convergence theorem, *Amer. Math. Monthly* **93**:5 (1986), 395–397.
6. J. Van Yzeren, de Moivre's and Fresnel's integrals by simple integration, *Amer. Math. Monthly* **86**:8 (1979), 690–693.

A Publishing Paradox

Alert reader Jack C. Abad and his brother Victor Abad send the following:

> A recent Birkhäuser-Verlag book list included *Unpublished Philosophical Essays/Kurt Gödel*, edited by Francisco A. Rodriquez-Consuegra, 1995. If the title is accurate, it might make appropriate barbershop reading in that town where the barber shaves everyone who doesn't shave himself.

A quick search of Amazon.com turns up a wealth of similar material—unpublished recordings by Elizabeth Schwartzkopf and Marian Anderson, unpublished letters from General Robert E. Lee to Jefferson Davis, and unpublished opinions of the Warren Court. Author Michael McMullen is more scrupulously logical: The title of his book is *The Blessing of God: Previously Unpublished Sermons of Jonathan Edwards*.

PROBLEMS

Proposals

To be considered for publication, solutions should be received by July 1, 2005.

1711. *Proposed by Mowaffaq Hajja, Yarmouk University, Irbid, Jordan.*

In triangle ABC, let A' be on BC, B' on CA and A' on BC, and suppose that the cevians AA', BB', and CC' meet at M. Prove that if $\triangle ABC$ is similar to $\triangle A'B'C'$, then M is the centroid of $\triangle ABC$.

1712. *Proposed by William P. Wardlaw, U. S. Naval Academy, Annapolis, MD.*

For each integer $m > 1$, let $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ be the ring of integers modulo m, and let Z_m^* be the (multiplicative) group of units in Z_m. Find the sum $S(m) = \sum_{u \in \mathbb{Z}_m^*} u$ and the product $P(m) = \prod_{u \in \mathbb{Z}_m^*} u$ of all elements in Z_m^*.

1713. *Proposed by Shawn Hedman and David Rose, Florida Southern College, Lakeland, FL.*

Prove that

$$\sum_{n=4}^{\infty} \left(\sum_{k=2}^{n-2} \binom{n}{k}^{-1} \right) = \frac{3}{2}.$$

1714. *Proposed by Mohammed Aassila, Strasbourg, France.*

Let m, n, x, y, z be positive real numbers with $x + y + z = 1$. Prove that

$$\frac{x^4}{(mx+ny)(my+nx)} + \frac{y^4}{(my+nz)(mz+ny)} + \frac{z^4}{(mz+nx)(mx+nz)} \geq \frac{1}{3(m+n)^2}.$$

We invite readers to submit problems believed to be new and appealing to students and teachers of advanced undergraduate mathematics. Proposals must, in general, be accompanied by solutions and by any bibliographical information that will assist the editors and referees. A problem submitted as a Quickie should have an unexpected, succinct solution.

Solutions should be written in a style appropriate for this MAGAZINE. Each solution should begin on a separate sheet.

Solutions and new proposals should be mailed to Elgin Johnston, Problems Editor, Department of Mathematics, Iowa State University, Ames IA 50011, or mailed electronically (ideally as a LaTeX file) to ehjohnst@iastate.edu. All communications should include the readers name, full address, and an e-mail address and/or FAX number.

1715. *Proposed by Barthel Wayne Huff, Salt Lake City, UT.*

An urn contains 35 red balls, labeled 1, 2, ... , 35, and k blue balls. Balls are drawn one at a time at random, identified by number, then replaced, until a blue ball is drawn. Some red balls may be drawn more than once before the first blue is drawn. What is the minimal value of k for which the expected number of repetitions is less than 1?

Quickies

Answers to the Quickies are on page 73.

Q947. *Proposed by Robert Gregorac, Iowa State University, Ames, IA.*

Let

$$P_n(x) = x^n + x^{n-1} - x^{n-2} - x^{n-3} + x^{n-4} + \cdots \pm x \pm 1$$

be a polynomial with the pattern of sign changes indicated. (The last two terms depend on n modulo 4.) Prove that for $n \geq 4$, $P_n(x)$ must have at least one nonreal zero.

Q948. *Proposed by Yaroslav Krylyuk, Santa Fe Community College, Gainesville, FL.*

In $\triangle ABC$, angles B and C are acute and the altitude from A meets $\overline{BC}$ in K. Let M be an arbitrary point on $\overline{AK}$, let Q be the intersection of line BM with $\overline{AC}$, and let P be the intersection of line CM with $\overline{AB}$. Prove that $\angle PKA \cong \angle QKA$.

Solutions

A Positive Solution **February 2004**

1686. *Proposed by Shahin Amrahov, Ari College, Turkey.*

Find all positive integer solutions (x, y) to the equation

$$2y^2 = x^4 + 8x^3 + 8x^2 - 32x + 15.$$

Solution by Richard K. Guy, The University of Calgary, Alberta, Canada.

Since $2y^2$ is even, x is odd. Hence, $2y^2$ is a multiple of 8 and y is even. Substitute $x = 2X + 1$ and $y = 2Y$ to obtain

$$Y^2 = X(X+3)\big[2X(X+3) + 1\big]$$

As $X(X+3)$ and $2X(X+3)+1$ have no common factor other than 1, each is a square. But if $X > 1$, $X(X+3)$ lies strictly between $(X+1)^2$ and $(X+2)^2$ and so cannot be a square. So $X = 0$ or $X = 1$. The former choice leads to $y = 0$ and the latter to $x = 3$, $y = 12$, the only positive solution.

This completes the solution to the problem. Note, however, that if we write $x = v/(v-6)$ and $y = 6w/(v-6)^2$, then the equation becomes

$$w^2 = v^3 + v^2 - 84v + 270.$$

This is curve 1344Q1 in Cremona's tables. Its torsion points, ∞ and $(5, 0)$, correspond to $(1, 0)$ and $(-5, 0)$ on the original curve. The rank is 1 and a generator is $(9, 18)$, which corresponds to the solution $(3, 12)$. There are infinitely many rational solutions but, surprisingly, they are confined to the infinite component—there are none

on the loop shaped finite component. Correspondingly, the rational points on the original curve, whose axes of symmetry are $y = 0$ and $x = -2$, are dense on the infinite components and absent from the loop. Examples of such points on the original curve are $(-7, \pm 12)$ and $(269/119, \pm 101160/119^2)$.

Also solved by JPV Abad, Roy Barbara (Lebanon), Michel Bataille (France), Brian D. Beasley, Tom Beatty, J. C. Binz (Switzerland), Jean Bogaert (Belgium), Brain Bradie, Stan Byrd and Lucas Van der Merwe, Robert Calcaterra, Minh Can, Michael Caulfield, John Christopher, Con Amore Problem Group (Denmark), Charles K. Cook, Randall J. Covill, Knut Dale (Norway), Charles R. Diminnie, Daniele Donini (Italy), Robert L. Doucette, Ragnar Dybvik (Norway), Timothy Eckert, Habib Y. Far, Tim Flood, Kenneth Fogarty, John F. Goehl, Michael Goldenberg and Mark Kalpan, G.R.A.20 Problems Group (Italy), Brian Hogan, Tom Jager, Kenneth Korbin, Victor Y. Kutsenok, Elias Lampakis (Greece), Kee-Lai Lau (China), Peter W. Lindstrom, Robert S. Lubarsky, David E. Manes, Allen J. Mauney, Northwestern University Math Problem Solving Group, Rolf Richberg (Germany), Fary Sami, Heinz-Jürgen Seiffert (Germany), Raul A. Simon (Chile), Albert Stadler (Switzerland), Daniel Stock, Paul Weisenhorn (Germany), Chu Wenchang and Di Claudio Leontina Veliana (Italy), Doug Wilcock, Hongbiao Zeng, Li Zhou, and the proposer. There was one incorrect submission.

Please, You Go First **February 2004**

1687. *Proposed by Sung Soo Kim, Hanyang University, Ansan Kyunggi, Korea.*

A two-player game starts with two sticks, one of length n and one of length $n + 1$, where n is a positive integer. Players alternate turns. A turn consists of breaking a stick into two sticks of positive integer lengths, or removing k sticks of length k for some positive integer k. The player who makes the last move wins. Which player can force a win?

Solution by Li Zhou, Polk Community College, Winter Haven, FL.

Let A be the set of game positions with an even number of sticks and at most one stick of even length. Let B be the set of game positions with an odd number of sticks and at most two sticks of even length. Note that the initial and final game positions are in A. It is also evident that any move from a position in A results in a position in B, and that from each position in B a move can be made that results in a position in A. Thus the second player can force a win by always making a move that puts the game back into a position in A.

Also solved by JPV Abad, Roy Barbara (Lebanon), Jean Bogaert (Belgium), Glenn Bookhout, Con Amore Problem Group (Denmark), Timothy Eckert, David Gove, G.R.A.20 Problems Group (Italy), Jerrold W. Grossman, Richard K. Guy (Canada), Eric Harclerode, Tom Jager, Victor Y. Kutsenok, Robert S. Lubarsky, Jacob McMillen, Mike Pinter, Robert P. Sealy, Harry Sedinger, Furman Smith, Jon Stadler, Patrick A. Staley, Paul Weisenhorn (Germany), Hongbiao Zeng, and the proposer. There was one incorrect submission.

A Leading Multiple of p **February 2004**

1688. *Proposed by Mihai Manea, Princeton University, Princeton, NJ.*

Let p be an odd prime, and let $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{p-1}x^{p-1}$ be a polynomial of degree $p - 1$ with integral coefficients. Suppose that $p \nmid (P(b) - P(a))$ whenever a and b are integers such that $p \nmid (b - a)$. Prove that $p \mid a_{p-1}$.

Solution by David Gove, California State University Bakersfield, Bakersfield, CA.

Because $a \not\equiv b \pmod{p}$ implies $P(a) \not\equiv P(b) \pmod{p}$, it follows that $P(0)$, $P(1)$, $\ldots$, $P(p-1)$ form a complete residue system modulo p. Thus

$$0 \equiv \sum_{i=0}^{p-1} i \equiv \sum_{j=0}^{p-1} P(j) \equiv pa_0 + \sum_{k=1}^{p-1} a_k \left(\sum_{j=0}^{p-1} j^k \right) \pmod{p}. \qquad (*)$$

To evaluate the inner sum consider two cases. If $k = p - 1$, then by Fermat's Theorem,

$$\sum_{j=0}^{p-1} j^k \equiv \sum_{j=1}^{p-1} 1 \equiv p - 1 \pmod{p}.$$

If $1 \le k \le p-2$, let g be a generator of the multiplicative group $\mathbb{Z}_p \backslash \{0\}$. Then

$$S_k = \sum_{j=0}^{p-1} j^k \equiv \sum_{m=1}^{p-1} (g^m)^k \equiv \sum_{m=1}^{p-1} (g^k)^m \pmod{p},$$

so

$$g^k S_k \equiv \sum_{m=1}^{p-1} (g^k)^{m+1} \equiv \sum_{m=2}^{p} (g^k)^m \equiv \sum_{m=1}^{p-1} (g^k)^m \equiv S_k \pmod{p}.$$

Because $g^k \not\equiv 1 \pmod{p}$, it follows that $S_k \equiv 0 \pmod{p}$. Using these results in $(*)$ we find

$$0 \equiv (p-1)a_{p-1} \pmod{p},$$

and it follows that $p \mid a_{p-1}$.

Also solved by JPV Abad, Fernando Barrera (Mexico), Michel Bataille (France), John Christopher, Con Amore Problem Group (Denmark), Daniele Donini (Italy), Robert L. Doucette, Michael Goldenberg and Mark Kaplan, Tom Jager, Peter W. Lindstrom, Rolf Richberg (Germany), Albert Stadler (Switzerland), H. T. Tang, Paul Weisenhorn (Germany), Chu Wenchang (Italy), Li Zhou, and the proposer.

Three Points and a Cosine **February 2004**

1689. *Proposed by Ali Nabi Duman, student, Bilkent University, Ankara, Turkey.*

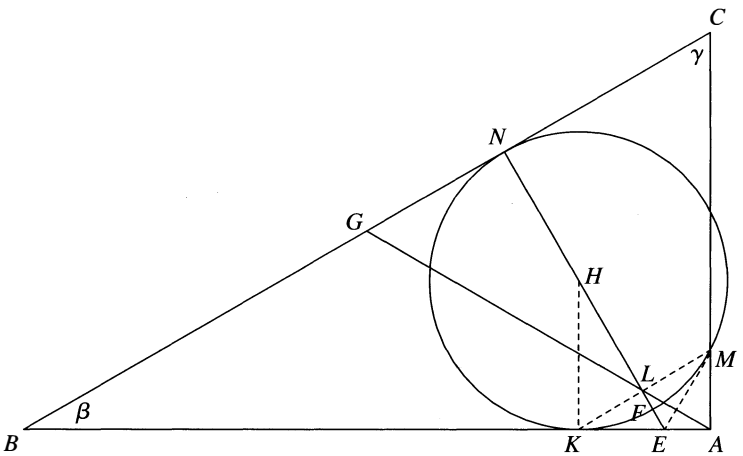
Triangle ABC is a right triangle with right angle at A. Circle $\mathcal{C}$ is tangent to $\overline{AB}$ and $\overline{BC}$ at K and N, respectively, and intersects $\overline{AC}$ in points $M(\neq A)$ and P, with $AM < AP$. The line perpendicular to $\overline{BC}$ at N intersects the median from A, the circle $\mathcal{C}$, and $\overline{AB}$ in points L, F, and E, respectively. Prove that if $FL/EF = LN/EN$, then

a. K, L, and M are collinear.

b. $\cos(2\angle ABC) = EA/EK$.

Solution by Paul Weisenhorn, Fautenbach, Germany.

a. The points N, L, F, E lie on a diameter. Because $FL/EF = LN/EN$, the points E and L divide NF harmonically. Thus, taking E as a pole, the corresponding polar line, with respect to $\mathcal{C}$, is $\overleftrightarrow{KL}$. This line is perpendicular to $\overline{NF}$, and hence parallel to $\overline{BC}$. Let the polar line intersect circle $\mathcal{C}$ in M_1 (in addition to K) and intersect $\overline{AC}$ in M_2. Then $KL/LM_2 = BG/GB = 1$, where G is the midpoint of $\overline{BC}$. Because $KL = LM_1$, it follows that $M_1 = M_2 = M$, and hence that K, L, M are collinear.



b. Let H be the center of $\mathcal{C}$, $\angle ABC = \beta$, and $\angle BCA = \gamma$. Then $\angle NHK = \pi - \beta$ and $\angle KHE = \beta = \angle EHM$. Thus $\angle HEK = \gamma = \angle HEM$ and it follows that $\angle AEM = \pi - \angle MEK = \pi - 2\gamma = 2\beta$. Thus $\cos(2\beta) = EA/EM = EA/EK$.

Also solved by Michel Bataille (France), Peter J. Gressis, Raul A. Simon, Li Zhou, and the proposer. There was one imcomplete submission.

Confronting a Negative Identity **February 2004**

1690. *Proposed by Costas Efthimiou, Department of Physics, and Peter Hilton, Department of Mathematics, University of Central Florida, Orlando, FL.*

Prove that there exist functions $f : \mathbb{R} \to \mathbb{R}$ that satisfy

$$f\big(x - f(y)\big) = f(x) + y$$

for all $x, y \in \mathbb{R}$, and show how such functions can be constructed.

Solution by Eugene Herman, Grinnell College, Grinnell IA.

Consider $\mathbb{R}$ to be a vector space over the field of rationals $\mathbb{Q}$, and let $\{e_\alpha\}_{\alpha \in I}$ be an algebraic basis of $\mathbb{R}$ over $\mathbb{Q}$. Next partition the (uncountable) index set I into disjoint subsets J and K of equal cardinality, and let β be a bijection from J onto K. We can construct a function f that satisfies the functional equation as follows. First, define f on the basis $\{e_\alpha\}_{\alpha \in I}$ by

$$f(e_\alpha) = \begin{cases} e_{\beta(\alpha)} & \alpha \in J \\ -e_{\beta^{-1}(\alpha)} & \alpha \in K, \end{cases}$$

then extend f to all of $\mathbb{R}$ by linearity. Note that $f\,(f(e_\alpha)) = -e_\alpha$ for all $\alpha \in I$. Therefore

$$f \text{ is a linear transformation on } \mathbb{R} \text{ such that } f \circ f = -i, \qquad (*)$$

where i is the identity function. Such a function satisfies the functional equation because

$$f\big(x - f(y)\big) = f(x) - f\big(f(y)\big) = f(x) + y.$$

For completeness, we include a proof that any function satisfying the functional equation also satisfies $(*)$. We first show that $f(0) = 0$. Setting $x = y = 0$ in the functional equation gives $f(-f(0)) = f(0)$. Then letting $x = 0$, $y = -f(0)$ leads to

$$0 = f\Big(-f\big(-f(0)\big)\Big) = f\big(-f(0)\big) = f(0).$$

Now let $x = f(y)$ in the functional equation. Because $f(0) = 0$, we have $f(f(y)) = -y$ for all $y \in \mathbb{R}$, that is, $f \circ f = -i$. Thus, for all $x, y \in \mathbb{R}$, we have

$$f(x + y) = f\Big(x - f\big(f(y)\big)\Big) = f(x) + f(y).$$

Because f is additive, it is linear over Q, showing that f satisfies $(*)$.

Also solved by John A. Baker (Canada), Roy Barbara (Lebanon), Michel Bataille (France), Natasha Borjemscaia, Con Amore Problem Group (Denmark), Randall J. Covill, A. K. Desai (India), Daniele Donini (Italy), Bruce Ebanks, David Gove, Tom Jager, Northwestern University Math Problem Solving Group, Albert Stadler (Switzerland), Li Zhou, and the proposer. There was one incorrect submission and one incomplete submission.

Answers

Solutions to the Quickies from page 69.

A947. The form of $P(x)$ reminds us of a geometric sum, suggesting that we investigate a product

$$A_n(x) = P_n(x)(x^2 + 1) = x^{n+2} + x^{n+1} \pm x \pm 1.$$

Applying Descartes' rule of signs to each of the four possibilities shows that A_n has at most four real zeros, and hence that P_n has at least $n - 4$ complex zeros. In particular, if $n \geq 5$, then P_n has at least one complex zero. Finally,

$$P_4(x) - 1 = x^4 + x^3 - x^2 - x = x(x - 1)(x + 1)^2$$

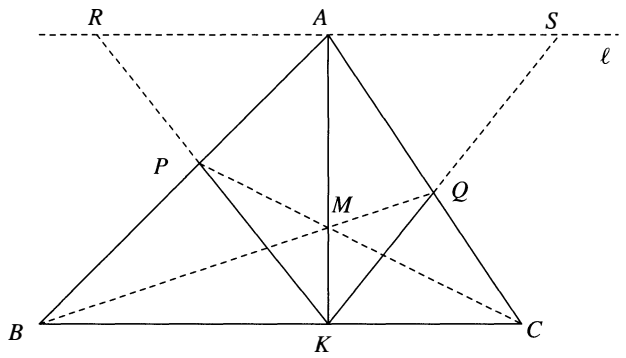
has a local minimum at the double zero $x = -1$ and an absolute minimum between the zeros 0 and 1. It follows that P_4 has at most two real zeros. This completes the proof.

A bit more can be discovered about A_n when n is odd. For such n,

$$A_n(x) = (x + 1)(x^{n+1} \pm 1).$$

If the $+$ sign is in effect, then we see that the only real zero for P_n is -1. If the $-$ sign in in effect, then P_n has real zeros $-1, -1, 1$, listed by multiplicity.

A948. Let ℓ be the line through A and parallel to $\overline{BC}$, and let R and S denote, respectively, the points at which the extensions of $\overline{KP}$ and $\overline{KQ}$ intersect ℓ.



It suffices to prove that $RA = SA$. By Ceva's Theorem,

$$\frac{BP}{PA} \cdot \frac{AQ}{QC} \cdot \frac{CK}{KB} = 1. \qquad (*)$$

Because $\triangle KBP \sim \triangle RPA$, we have $\frac{BP}{PA} = \frac{KB}{AR}$, and $\frac{AQ}{QC} = \frac{AS}{CK}$ follows by similar reasoning. Substituting these results into $(*)$ we obtain

$$\frac{KB}{AR} \cdot \frac{AS}{CK} \cdot \frac{CK}{KB} = 1,$$

and $AR = AS$ follows.

EDITOR'S NOTE: Please see "A Note from the Problems Editor" on p. 44.

REVIEWS

PAUL J. CAMPBELL, *Editor*
Beloit College

Assistant Editor: Eric S. Rosenthal, West Orange, NJ. Articles and books are selected for this section to call attention to interesting mathematical exposition that occurs outside the mainstream of mathematics literature. Readers are invited to suggest items for review to the editors.

ISIS Symmetry CD. International Society for the Interdisciplinary Study of Symmetry. $45 (postpaid) (e-mail `jablans@mi.sanu.ac.yu` and send check to Slavik Jablan, The Mathematical Institute, Knez Mihailova 35, P.O. Box 367, 11001 Belgrade, Yugoslavia).

This CD contains the first 10 issues of the electronic journal *Visual Mathematics* (`http://members.tripod.com/vismath/vm.htm`), which is a supplement to the printed journal *Symmetry: Art and Science*, plus further materials about symmetry in music and three complete books. The books are Naomi Asakura's *Fundamental Problems in Creating in Two-Dimensional Space* (translated from Japanese, with 700 illustrations), Erno Lendvai's *Symmetries of Music* (in English and in German), and Slavik Jablan's *Symmetry and Ornament*. If you need some eye candy to interest people in mathematics, this CD and *Visual Mathematics* itself (plus the fractals book/film below) are great sources.

Clarke, Arthur C., et al., *The Colours of Infinity: The Beauty and Power of Fractals*, with zone-free PAL-format DVD containing *Arthur C. Clarke's Colours of Infinity* (50 min), a Nigel Lesmoir-Gordon film produced by Paul Sinclair with music by David Gilmour (of Pink Floyd), and *Infinit* (30 min), a Nigel Lesmoir-Gordon "chillout film" produced by Paul Benson, with music by The Infinity Project and Total Eclipse. Clear Books, 2004; 176 pp, $29.95 (P). ISBN 1–904555–05–5. (Caution: The DVD plays on all computers but not on most U.S. DVD players; a U.S. edition with NTSC DVD is planned.)

This book celebrates the 10th anniversary of a film that you may have missed at the time (as I did), the 80th birthday of Benoît Mandelbrot, and the 30th birthday of the word "fractal." The book presents original exposition and reflection on fractals by their foremost exponents, including Ian Stewart, Arthur C. Clarke, Michael Barnsley, and Mandelbrot himself, who are the principals in the film (whose shooting script is reproduced too). The exposition (which has only one serious equation) and the illustrations in the book are wonderful; I particularly liked Barnsley's "soccer game" approach to generating fractals. The film includes zooms in and out of the Mandelbrot set, through dozens of orders of magnitude. I was surprised to learn that the film's music and images "have become club and garage favourites" (the "chillout" supplemental film does remind me of the psychedelicism of the 1960s).

Hufnagel L., D. Brockmann, and T. Geisel, Forecast and control of epidemics in a globalized world, *Proceedings of the National Academy of Sciences* 101 (42) (19 October 2004) 15124–15129. `www.pnas.org/cgi/doi/10.1073/pnas.0308344101` .

The authors model contemporary dispersion of infectious diseases through global human travel. Their accompanying simulation of the spread of SARS (severe acute respiratory syndrome) is eerily accurate. They examine the influence of vaccination and of travel restrictions; whether governments can respond fast enough and would make the necessary tough decisions (e.g., isolate large cities) is questionable.

Felten, Edward W., Aviel D. Rubin, and Adam Stubblefield, Analysis of voting data from the recent Venezuela referendum [*disponible en español también*], `http://www.venezuela-referendum.com/` .

Apart from its uses in predicting the results of an election, probability can have a role in checking the results: Certain kinds of election fraud are likely to produce statistical anomalies. In August, Venezuela held a referendum; its president Hugo Chávez won with 58% of the votes, but the opposition suspected tampering because in some precincts the same numbers of "yes" votes or "no" votes were recorded on several voting machines. Could this have happened by coincidence? Was the number of "yes" votes per machine "capped" by the vote-counting program? The computer scientist authors simulated the election 1,238 times and found no stark statistical anomalies. "Our results, at most, can shed light on whether certain types of fraud occurred; but an analysis like ours cannot rule out fraud altogether." (Thanks to George Szpiro of the *Neue Zürcher Zeitung* (Switzerland).)

Dorsey-Palmateer, Reid, and Gary Smith, Bowlers' hot hands, *American Statistician* 58 (1) (February 2004) 38–45.

Whether the phenomenon of the "hot hand" exists—that some players in sports go on success streaks longer and more often than chance would suggest—may be a matter of "religious" belief, meaning that believers in it (including one member of my department) admit no falsifiability: They will continue to believe in the face of any contrary claims or data. Originally disputed in the context of basketball, the "hot hand" question is investigated in this article in the more controlled environment of professional bowling, which the authors consider "free of confounding influences." They find that the probability of rolling a strike is not independent of previous rolls and that the number of strikes rolled varies more across games than a binomial model would allow; and they cite an article in the psychology literature with similar findings for horseshoe pitching.

Albert, Jim, Streakiness in team performance, *Chance* 17 (3) (2004) 37–43.

A players is said to have a "hot hand" (or "be in a slump"), but when such a phenomenon occurs with a team, pundits say the team is "streaky." Author Albert investigates how to interpret the phenomenon of a 20-game winning streak in baseball (Oakland Athletics in 2002). He proposes a measure of consistency of performance and a model for team ability; he then simulates many seasons and the 2002 season in particular. The conclusion is: We should expect to see a streak of 20 or more games about once every 25 years.

Brooks, Michael, Return of a "beautiful mind," *New Scientist* (18 December 2004) 46–48; `http://www.newscientist.com/channel/opinion/mg18424781.800` .

This is the text of an interview with John Nash, who is questioned mainly about mental illness. He refers to his recovery as a "return" rather than a "rebirth," and hopes for a similar return for his afflicted mathematician son.

Weiss, Rick, Computer analysis is bringing science to art, *Washington Post* (29 November 2004), A8; `http://www.washingtonpost.com/wp-dyn/articles/A18423-2004Nov28.html` . Eisenberg, Anne, Who really wielded the paintbrush, *New York Times* (23 December 2004) E1, E11; `http://www.nytimes.com/2004/12/23/arts/23scan.html` . Lyu, Siwei, Daniel Rockmore, and Hany Farid, A digital technique for art authentication, *Proceedings of the National Academy of Sciences* 101 (2004) 17006–17010; `http://www.cs.dartmouth.edu/~farid/publications/pnas04.pdf` .

Wavelets can be compress an image; can they also characterize the paintings of an Old Master? After all, wavelets "assess graphical elements on many scales at once." A team at Dartmouth College, which previously used wavelets to detect tampering of a digital image, here uses it to assess eight paintings by Pieter Bruegel the Elder (1525/35–1569) and five acknowledged imitations. Their method shows a distinct separation (in 72-dimensional space) between the two groups (but I would have preferred separate training and test data sets). Says author Farid, "This is a great field, because no one can prove us wrong."

65th Annual William Lowell Putnam Mathematical Competition

Editor's Note: Additional solutions will be printed in the *Monthly* later in the year.

Problems

A1 Basketball star Shanille O'Keal's team statistician keeps track of the number, $S(N)$, of successful free throws she has made in her first N attempts of the season. Early in the season, $S(N)$ was less than 80% of N, but by the end of the season, $S(N)$ was more than 80% of N. Was there necessarily a moment in between when $S(N)$ was *exactly* 80% of N?

A2 For $i = 1, 2$, let T_i be a triangle with side lengths a_i, b_i, c_i, and area A_i. Suppose that $a_1 \leq a_2$, $b_1 \leq b_2$, $c_1 \leq c_2$, and that T_2 is an acute triangle. Does it follow that $A_1 \leq A_2$?

A3 Define a sequence $\{u_n\}_{n=0}^{\infty}$ by $u_0 = u_1 = u_2 = 1$, and thereafter by the condition that

$$\det \begin{pmatrix} u_n & u_{n+1} \\ u_{n+2} & u_{n+3} \end{pmatrix} = n!$$

for all $n \geq 0$. Show that u_n is an integer for all n. (By convention, $0! = 1$.)

A4 Show that for any positive integer n there is an integer N such that the product $x_1 x_2 \cdots x_n$ can be expressed identically in the form

$$x_1 x_2 \cdots x_n = \sum_{i=1}^{N} c_i \, (a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n)^n$$

where the c_i are rational numbers and each a_{ij} is one of the numbers -1, 0, 1.

A5 An $m \times n$ checkerboard is colored randomly: each square is independently assigned red or black with probability 1/2. We say that two squares, p and q, are in the same connected monochromatic region if there is a sequence of squares, all of the same color, starting at p and ending at q, in which successive squares in the sequence share a common side. Show that the expected number of connected monochromatic regions is greater than $mn/8$.

A6 Suppose that $f(x, y)$ is a continuous real-valued function on the unit square $0 \leq x \leq 1$, $0 \leq y \leq 1$. Show that

$$\int_0^1 \left(\int_0^1 f(x, y)\, dx \right)^2 dy + \int_0^1 \left(\int_0^1 f(x, y)\, dy \right)^2 dx$$
$$\leq \left(\int_0^1 \int_0^1 f(x, y)\, dx\, dy \right)^2 + \int_0^1 \int_0^1 f(x, y)^2\, dx\, dy.$$

B1 Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integral coefficients. Suppose that r is a rational number such that $P(r) = 0$. Show that the $n+1$ numbers

$$a_n, \quad a_n r + a_{n-1}, \quad a_n r^2 + a_{n-1}r + a_{n-2}, \ldots, a_n r^n + a_{n-1}r^{n-1} + \cdots + a_0$$

are integers.

B2 Let m and n be positive integers. Show that

$$\frac{(m+n)!}{(m+n)^{m+n}} < \frac{m!}{m^m} \cdot \frac{n!}{n^n}.$$

B3 Determine all real numbers $a > 0$ for which there exists a nonnegative continuous function $f(x)$ defined on $[0, a]$ with the property that the region

$$R = \{(x, y) : 0 \le x \le a,\ 0 \le y \le f(x)\}$$

has perimeter k units and area k square units for some real number k.

B4 Let n be a positive integer and $\theta = 2\pi/n$. Define points $P_k = (k, 0)$ in the xy-plane, for $k = 1, 2, \ldots, n$. Let R_k be the map that rotates the plane counterclockwise by the angle θ about the point P_k. Let R denote the map obtained by applying, in order, R_1, then R_2, ..., then R_n. For an arbitrary point (x, y), find, and simplify, the coordinates of $R(x, y)$.

B5 Evaluate

$$\lim_{x \to 1^-} \prod_{n=0}^{\infty} \left(\frac{1 + x^{n+1}}{1 + x^n} \right)^{x^n}.$$

B6 Let $\mathcal{A}$ be a non-empty set of positive integers, and let $N(x)$ denote the number of elements of $\mathcal{A}$ not exceeding x. Let $\mathcal{B}$ denote the set of positive integers b that can be written in the form $b = a - a'$ with $a \in \mathcal{A}$ and $a' \in \mathcal{A}$. Let $b_1 < b_2 < \cdots$ be the members of $\mathcal{B}$, listed in increasing order. Show that if the sequence $b_{i+1} - b_i$ is unbounded, then $\lim_{x \to \infty} N(x)/x = 0$.

Solutions

Solution to A1 Yes. Consider the integer-valued function, $f(N) = 5S(N) - 4N$. The hypotheses then say that there are integers N_1 and N_2 with $1 \le N_1 < N_2$ and $f(N_1) < 0 < f(N_2)$. Define N to be the first integer after N_1 such that $0 \le f(N)$. Compute the difference

$$f(N) - f(N-1) = 5 \cdot \big(S(N) - S(N-1)\big) - 4.$$

Note that this function has only two values, $+1$ when the shot is made and -4 when a shot is missed. In order for $f(N-1)$ to be negative and $f(N)$ nonnegative, O'Keal must have made the Nth shot, which means $f(N) = 0$. Rewriting gives $S(N)/N = 4/5 = 80\%$.

Solution to A2 Yes. Let $\alpha_i, \beta_i, \gamma_i$ be the angles opposite sides a_i, b_i, c_i, for $i = 1, 2$. Since $\alpha_i + \beta_i + \gamma_i = \pi$ for $i = 1, 2$, it follows that at least one of the inequalities $\alpha_1 \le \alpha_2$, $\beta_1 \le \beta_2$, $\gamma_1 \le \gamma_2$ must hold. Without loss of generality, $\alpha_1 \le \alpha_2$. But $\alpha_2 \le \pi/2$, and $\sin x$ is increasing on $[0, \pi/2]$, so

$$A_1 = \frac{1}{2} b_1 c_1 \sin\alpha_1 \le \frac{1}{2} b_2 c_2 \sin\alpha_2 = A_2.$$

Solution to A3 We show that for $n > 0$,

$$u_n = (n-1)!! = \begin{cases} (n-1)(n-3)\cdots 3\cdot 1 & \text{if } n \text{ is even,} \\ (n-1)(n-3)\cdots 4\cdot 2 & \text{if } n \text{ is odd,} \end{cases}$$

taking $0!! = 1$. Note that for all $n > 0$, $n! = (n-1)!!\,n!!$ and $(n+1)!! = (n+1)\cdot(n-1)!!$.

We solve the determinant condition for u_{n+3} in terms of u_n, u_{n+1}, u_{n+2} to get the recurrence

$$u_{n+3} = (n! + u_{n+1}u_{n+2})/u_n.$$

Since then $u_3 = 2$, $u_4 = 3$, $u_5 = 8 = 4\cdot 2$, and $u_6 = 15 = 5\cdot 3$, we see that the assertion is correct for the first several cases. Assume that $n+3 > 6$ and suppose that $u_n = (n-1)!!$, $u_{n+1} = n!!$ and $u_{n+2} = (n+1)!!$. Then

$$\begin{aligned} u_{n+3} &= \frac{n! + n!!\,(n+1)!!}{(n-1)!!} = \frac{(n-1)!!\,n!! + n!!\,(n+1)(n-1)!!}{(n-1)!!} \\ &= (n+2)\cdot n!! = (n+2)!! \end{aligned}$$

so the result follows by induction.

Solution to A4 (by Kiran Kedlaya and Lenny Ng) It suffices to verify that

$$2^n n! x_1 \cdots x_n = \sum_{e_i \in \{-1,1\}} (e_1 \cdots e_n)(e_1 x_1 + \cdots + e_n x_n)^n.$$

To check this, first note that the right side vanishes identically for $x_1 = 0$, because each term cancels the corresponding term with e_1 negated; similarly, it is divisible by $x_2, \ldots, x_n$. Thus, the right-hand side is equal to a constant times $x_1 \cdots x_n$. Since there are 2^n summands and each contributes $n!$ copies of $x_1 \cdots x_n$, the constant is $2^n n!$.

Solution to A5 Label the squares 1 to mn, by row, from the bottom to the top and within rows from left to right. Let R_i represent the number of connected monochromatic regions, considering only the first i squares. A single square must be monochromatic, so the expected value $\mathrm{E}(R_1)$ is 1. For $2 \le i \le n$, and for $i \equiv 1 \mod n$, with $i > 1$ (the bottom row and the left edge), the odds are even that $R_i - R_{i-1}$ is 0 or 1. Otherwise, $R_i - R_{i-1}$ can be $-1, 0$ or 1. Consider the colors of the squares labeled i, $i-1$, $i-n$, $i-n-1$. Of the 16 ways to color these squares, two of these may result in a monochromatic region counted in R_i that breaks into two regions in R_{i-1}, namely, when all the squares are the same, except the one labeled $i-n-1$; however, looking outside these four squares, we see that some such configurations do not break. This means that $R_i - R_{i-1} = -1$ with probability strictly less than $1/8$. Similarly, if square i differs from squares $i-1$ and $i-n$ (which happens with probability $1/4$), then $R_i - R_{i-1} = 1$. In all other cases, this difference is 0. Thus, the expected value of the difference is

$$\mathrm{E}(R_i - R_{i-1}) > \frac{1}{4}\cdot 1 + \frac{1}{8}\cdot(-1) = \frac{1}{8}.$$

Summing gives $\mathrm{E}(R_j) > j/8$ for all j. Put $j = mn$ for the desired result.

Solution to A6 The right hand side minus the left hand side can be seen to equal

$$\frac{1}{4}\int_0^1\int_0^1\int_0^1\int_0^1 \big(f(x_1,y_1) - f(x_1,y_2) - f(x_2,y_1) + f(x_2,y_2)\big)^2\, dx_1 dx_2\, dy_1 dy_2.$$

Solution to B1 Let $r = p/q$ in lowest terms for integers p and q, and let

$$S_k = a_n r^k + a_{n-1} r^{k-1} + \cdots + a_{n-k+1} r;$$

that is, $S_1 = a_n r$, and $S_k = (S_{k-1} + a_{n-k+1})r$, for $1 < k \leq n$.

Note that $S_n + a_0 = P(r) = 0$, so $S_n = -a_0$ is an integer. We'll prove the result by inducting downward on k.

Suppose that S_k is an integer and let

$$Q_k(x) = a_n x^k + a_{n-1} x^{k-1} + \cdots + a_{n-k+1} x - S_k.$$

Then $Q_k(x)$ is a polynomial with integer coefficients and $Q(p/q) = 0$. Thus, by the Rational Root Theorem, p divides the constant term S_k, and therefore $S_{k-1} = qS_k/p - a_{n-k+1}$ is an integer. This completes the proof.

Solution to B2 (Submitted by a contestant) Consider a string of code with length $m + n$ in which each position can be a number from 1 to $m + n$. The number of possible codes is $(m + n)^{m+n}$. However, let us construct code strings by the following method: Select m positions from the string. Fill these m positions using only the numbers 1 through m. In the other n positions, use only numbers from $m + 1$ through $m + n$. The number of ways to do this is $\binom{m+n}{n} \cdot m^m \cdot n^n$. This method cannot cover all the possible codes. For instance, a string of 1s would not be possible. Thus

$$\binom{m+n}{n} \cdot m^m \cdot n^n < (m+n)^{m+n} \quad \text{and so} \quad \frac{(m+n)!}{(m+n)^{m+n}} < \frac{m!}{m^m} \cdot \frac{n!}{n^n}.$$

Solution to B3 The answer is any real number greater than 2.

Because f is continuous on a closed interval, it attains a maximum value on that interval, say at $P = (c, M)$ for some c in $[0, a]$. ($M > 0$, for otherwise the degenerate region would have positive perimeter but zero area.) Clearly, R is bounded above by the rectangle over $[0, a]$ of height M, so that area $k \leq aM$. On the other hand, $2M < k$, since $2M$ is less than the sum of the distances from $(0, 0)$ to P and from P to $(a, 0)$, which in turn is smaller than the total perimeter k. It follows that $2M < aM$, so $a > 2$.

Conversely, if $a > 2$ we can take $f(x) = 2a/(a - 2)$. Then R is a rectangle with area $2a^2/(a - 2)$ and perimeter

$$2a + 2\left(\frac{2a}{a-2}\right) = \frac{2a^2}{a-2}.$$

Solution to B4 (by Andy Lutomirski, communicated by Ravi Vakil) Imagine a regular n-gon of side length 1 placed with its top edge on the x-axis and the left endpoint of that edge at the origin. Then the rotations correspond to rolling this n-gon along the x-axis. After the n rotations, it must end up in its original orientation, but translated n units to the right. Hence, the whole plane must do so as well.

Solution to B5 The limit is $2/e$.

For the moment, fix $x < 1$. Considering the left-hand and right-hand evaluations for the Riemann sum approximations to the integral of the increasing function $\ln(1 + x)$ on the interval $[0, 1]$, using the partition $0, x^n, x^{n-1}, \ldots, x, 1$, we see that when x is large enough so that $x^n < 1 - x$,

$$\sum_{i=1}^{n} (x^{i-1} - x^i) \ln(1 + x^i) < \int_0^1 \ln(1 + x)\, dx$$

$$< \sum_{i=1}^{n} (x^{i-1} - x^i) \ln(1 + x^{i-1}) + (1 - x) \ln 2.$$

As $n \to \infty$, the sum on the left increases and is bounded above, and therefore it converges to a sum that is less than or equal to the integral. Now letting x approach 1 from below we find

$$\lim_{x\to 1^-} \sum_{i=1}^{\infty} (x^{i-1} - x^i) \ln(1 + x^i) = \int_0^1 \ln(1 + x)\, dx = 2\ln 2 - 1.$$

Exponentiating gives

$$\lim_{x\to 1^-} \prod_{i=1}^{\infty} (1 + x^i)^{(x^{i-1}-x^i)} = e^{2\ln 2 - 1} = \frac{4}{e},$$

and therefore

$$\lim_{x\to 1^-} \prod_{i=0}^{\infty} \left(\frac{1 + x^{i+1}}{1 + x^i}\right)^{x^i} = \lim_{x\to 1^-} \left(\frac{1 + x^1}{1 + 1}\right)^1 \left(\frac{1 + x^2}{1 + x^1}\right)^{x^1} \left(\frac{1 + x^3}{1 + x^2}\right)^{x^2} \cdots$$

$$= \lim_{x\to 1^-} \frac{1}{1 + 1} \prod_{i=1}^{\infty} (1 + x^i)^{(x^{i-1}-x^i)} = \frac{1}{2}\left(\frac{4}{e}\right) = \frac{2}{e}.$$

Solution to B6 Put $d = \lim_{x\to\infty} N(x)/x$. If every nonnegative integer is in $\mathcal{B}$ then $b_{i+1} - b_i = 1$ for all i, which is a bounded sequence. Suppose there is a positive integer c_1 not in $\mathcal{B}$. Then, for each $a \in \mathcal{A}$, the number $a + c_1$ is not in $\mathcal{A}$. Hence $d \le 1/2$. Suppose now that the sequence b_i has a gap of length $> 2c_1$. Let c_2 be an integer in the middle of this gap, so that $c_2 - c_1$, c_2, $c_2 + c_1$ lie in the gap. Thus none of these three numbers is in $\mathcal{B}$, and hence for any $a \in \mathcal{A}$, the three numbers $a + c_1$, $a + c_2$, $a + c_1 + c_2$ do not lie in $\mathcal{A}$. Note also that if a' is a second member of $\mathcal{A}$, then the numbers $a' + c_1$, $a' + c_2$, $a' + c_2 + c_1$ eliminated by a' are distinct from the three numbers eliminated by a, for if one of the numbers from the first list is equal to one of the numbers in the second, then $\pm(a - a')$ is one of the numbers c_1, $c_2 - c_1$, c_2, or $c_2 + c_1$, a contradiction. Since each $a \in \mathcal{A}$ eliminates three numbers, and since the numbers eliminated are disjoint for distinct a, it follows that $d \le 1/4$. We continue by induction. Suppose that $c_1, \ldots, c_{k-1}$ have been chosen so that no number of the form $c_j + \varepsilon_{j-1}c_{j-1} + \cdots \varepsilon_1 c_1$ is in $\mathcal{B}$, where $1 \le j < k$ and $\varepsilon_i \in \{-1, 0, 1\}$. Suppose that $\mathcal{B}$ contains a gap more than twice as long as $c_1 + c_2 + \cdots + c_{k-1}$, and let c_k be a number in the middle of this gap, so that no number of the form $c_k + \varepsilon_{k-1}c_{k-1} + \cdots + \varepsilon_1 c_1$ is in $\mathcal{B}$. If $a \in \mathcal{A}$, then none of the $2^k - 1$ numbers $a + \delta_1 c_1 + \delta_2 c_2 + \cdots + \delta_k c_k$ is in $\mathcal{A}$, where $\delta_i \in \{0, 1\}$ for $1 \le i \le k$ with not all $\delta_i = 0$. Moreover, the numbers eliminated by $a \in \mathcal{A}$ are disjoint from the numbers eliminated by $a' \in \mathcal{A}$. To see this, suppose that

$$a + \delta_1 c_1 + \cdots + \delta_k \delta_k = a' + \delta_1' c_1 + \cdots + \delta_k' c_k.$$

If $\delta_i = \delta_i'$ for all i then $a = a'$. Otherwise, there is an i such that $\delta_i \ne \delta_i'$. Let j be the largest such integer. By interchanging a and a', if necessary, we may suppose that $\delta_j = 0$, $\delta_j' = 1$. Then

$$a - a' = c_j + \varepsilon_{j-1}c_{j-1} + \cdots + \varepsilon_1 c_1$$

where $\varepsilon_i = \delta_i' - \delta_i \in \{-1, 0, 1\}$. Since no number of this form is in $\mathcal{B}$, this is impossible. As each $a \in \mathcal{A}$ eliminates $2^k - 1$ other numbers, it follows that $d \le 1/2^k$. Thus we see that if $\mathcal{B}$ contains gaps of arbitrarily great length, then $d = 0$.

Thanks to Byron Walden for editorial assistance.

CONTENTS

ARTICLES

3 Fermat: The Founder of Modern Number Theory, *by Israel Kleiner*

14 Proof Without Words: Pythagorean Triples and Factorizations of Even Squares, *by José A. Gomez*

15 The Singled Out Game, *by Kennan Shelton*

26 Height and Excess of Pythagorean Triples, *by Darryl McCullough*

NOTES

45 Hidden Group Structure, *by Ruth I. Berger*

48 The St. Basil's Cake Problem, *by Christina Savvidou*

51 Replacement Costs: The Inefficiencies of Sampling with Replacement, *by Emily S. Murphree*

57 Can the Committee Meet? A Markov Chain Analysis, *by Terry L. Kiser, Thomas A. McCready, and Neil C. Schwertman*

63 Dirichlet and Fresnel Integrals via Iterated Integration, *by Paul A. Loya*

PROBLEMS

68 Proposals 1711–1715

69 Quickies 947–948

69 Solutions 1686–1690

73 Answers 947–948

REVIEWS

74

NEWS AND LETTERS

76 65th Annual William Lowell Putnam Mathematical Competition

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, DC 20036