Vol. 78, No. 3, June 2005

MATHEMATICS MAGAZINE

- In the Shadow of Giants: A Section of American Mathematicians, 1925–1950
- Farmer Ted Goes 3D
- Pythagorean Triples and Inner Products

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: *Wafer in a Shadow Box*, by Stephanie Haney.

The largest circle that fits inside a cube is inscribed in the hexagonal cross-section that is perpendicular to a main diagonal. "Wafer in a Box" by John E. Wetzel tells the general story of which this is a special case. Decorating the box are photographs of five mathematicians important in the early days of the Philadelphia Section of the MAA: John Robert Kline on the back left; Arnold Dresden on the back right; Joseph B. Reynolds on the right front; Albert A. Bennett on the left front; and Howard Hawks Mitchell on the bottom. Read "In the Shadow of Giants" by David E. Zitarelli to learn more about them.

Stephanie Haney is a student of photography at West Valley College, where Jason Challas supervised her work on this image. She will continue her studies at San Jose State University next fall. When not boxed in doing homework, Stephanie may be found at the movies 'til the wee hours of the morning.

AUTHORS

David Zitarelli has had two careers as a mathematician, disjoint so far, first as an algebraist (semigroups) after receiving his Ph.D. at Penn State, and then as a historian after he moved to Temple University. His involvement with both institutions has enabled him to learn about teaching from two different kinds of institutions, Joe Paterno (football) and John Chaney (basketball). The present article evolved from research carried out since the publication of his book on the history of an MAA section, which was viewed as a microcosm of mathematics in America during 1925–2001.

Shawn Alspaugh is a VIGRE fellowship recipient in the doctoral program at Indiana University in Bloomington, Indiana. In 2002, he graduated from Taylor University in Upland, Indiana, with a Bachelor of Science degree in mathematics education, and he is currently licensed by the Indiana Department of Education. *Farmer Ted Goes 3D* is a product of research completed in the summer of 1999, supported by the Taylor University Science Research Training Program. Shawn's current mathematical interests are in the field of algebra. Outside of mathematics, Shawn enjoys waterskiing, swing dancing, basketball, and joking about not having a spleen.

Larry Gerstein received his Ph.D. in 1967 from the University of Notre Dame under the direction of Timothy O'Meara. His mathematical interests are in algebra and number theory, and his research has been primarily in the theory of quadratic forms. He has been at UCSB since 1967, but he has also had visiting positions at MIT, Notre Dame, Harvard, and Dartmouth. He enjoys teaching at all levels and is the author of the textbook *Introduction to Mathematical Structures and Proofs*. His nonprofessional activities include playing the trombone and violin. He was quite good on both instruments when he was 15, and with practice he is still good for a 15-year-old.

Vol. 78, No. 3, June 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

In the Shadow of Giants: A Section of American Mathematicians, 1925–1950

DAVID E. ZITARELLI
Temple University
Philadelphia, PA 19122
zit@temple.edu

Reading about giants in the history of mathematics can be exhilarating and rewarding. Here we expound on a group of five individuals who toiled in the shadows of American giants in the first half of the twentieth century. Our group consists of three who founded an MAA section (Joseph Reynolds, Howard Mitchell, and Albert Bennett) and two who nurtured the section during its infancy (J. R. Kline and Arnold Dresden). Although they made impressive contributions to the American mathematical community, they are not household names like three of the national figures who soared above them—E. H. Moore, Oswald Veblen, and R. L. Moore [**63**].

Yet our aim is much broader than describing the outstanding achievements of the early leaders of an MAA section. We uncover vital connections between our quintet and the national leaders that demonstrate how towering figures influence the rest of the mathematical community, thereby allowing us to better understand the dynamics of the interlocking pieces within the overall community. We also indicate how our five reflect major developments that took place within the American mathematical community during the second quarter of the 20th century. In addition, we glimpse their various philosophies on mathematics education during this period.

The paper begins with a brief history of AMS and MAA sections, including summaries of the founding of the Philadelphia Section (now called Eastern Pennsylvania and Delaware—EPADEL) and the establishment of this MAGAZINE by the Louisiana-Mississippi Section. Then we elucidate the lives and major works of the five mathematicians who were leaders locally but rank and file nationally. Along the way we indicate ways in which two of the MAA's official journals, the *American Mathematical Monthly* and this MAGAZINE, provided vital outlets for publishing this group's mathematical works and publicizing their views on mathematics education.

Sections

The MAA was founded on the last two days of 1915. By contrast, the AMS got its start in 1888 as the New York Mathematical Society. Initially the AMS was a local organization centered in New York, but the founding of three sections enabled it to spread its wings across the continent: Chicago in 1896, San Francisco in 1902, and Southwest in 1906. There was a much shorter gap between the birth of the MAA and the founding of its first sections—a matter of minutes. By the end of its first year, the MAA boasted six thriving sections; another ten would come on board in the next decade [**42**]. However, up to 1926 no section was located entirely in the East. (Two good sources on the early histories of the AMS and MAA are [**2**, pp. 3–9] and [**29**, pp. 18–21], respectively.)

Before then, MAA leaders Herbert Slaught and W. D. Cairns expressed concern about the "seeming apathy or lethargy" of mathematicians in the Atlantic States [**A1**]. That situation changed in 1925 when Joseph Reynolds of Lehigh University suggested the idea of forming a Lehigh Valley Section. However, Reynolds was unable to garner sufficient support for his idea. As Parshall and Rowe demonstrated so convincingly in their book *The Emergence of the American Mathematical Research Community*, every professional organization needs a sufficiently large *community* in order to survive, let alone thrive [**44**]. The missing piece to Reynolds's puzzle was a critical mass of individuals and institutions that would support his plan. He found them by looking south toward Philadelphia, a city whose population was approaching two million at the time.

On the Saturday after Thanksgiving in 1926, three individuals organized a meeting at Lehigh with the express purpose of forming an MAA section. To their delight, 20 members showed up and, after a morning of mathematical presentations, voted unanimously to petition the MAA to form the Philadelphia Section. At first MAA leadership opposed the name. As Albert Bennett wrote ([**A1**]; also recorded in [**42**, pp. 94–95]):

> At the organizational meeting... a request for establishing the Philadelphia section of the MAA was forwarded to Secretary Cairns. His first reaction was that the name was ill-chosen, since all the other Sections were named for States, and to name a section after so small a political unit as a city, would break sound precedent. I wrote back that Pennsylvania had two natural cultural centers, one at the extreme east (Philadelphia), the other at the extreme west (Pittsburgh). One could not expect much of an attendance at either of these places, from residents near the other. Philadelphia should attract persons from Eastern Pennsylvania, Delaware and southern New Jersey. Setting a new precedent might encourage the later founding of a Pittsburgh Section, attracting mathematical instructors from West Virginia and Eastern Ohio as well as from western Pennsylvania. Cairns and Slaught were not obstinate, and in December, the Section was admitted under its proposed name, subject of course to the usual provision of By-Laws, etc., and promises of good behavior.

We doubt whether the last part about "promises of good behavior" was actually stated. The author, Albert Bennett, a decidedly colorful personality with a gift for captivating prose, was one of the three founders of the section along with Howard Mitchell of the University of Pennsylvania (Penn) and Bennett's "ever loyal associate J. B. Reynolds" [**A1**]. Just as Bennett so presciently predicted, the Allegheny Section was formed at the other Pennsylvania focal point in 1933. Until then the Philadelphia Section included the central part of Pennsylvania, including active Penn State mathematicians. The section also included the southern part of New Jersey (including Rutgers and Princeton) up to the founding of the New Jersey Section in 1956 under Albert Meder of Rutgers and Albert W. Tucker of Princeton.

The Louisiana-Mississippi Section, established in 1924, two years before the Philadelphia Section, played a prominent role in the history of the MAGAZINE. We provide a synopsis of this development so the reader can place various events in historical perspective. (Beckenbach [**3**] provides a fuller treatment of the journal's history.) *Mathematics Magazine* began as a series of eight pamphlets written by Samuel Thomas Sanders (1872–1970) of Louisiana State University during 1926–27 to encourage membership in the MAA. Sanders's hope that the pamphlets could be expanded into a magazine was realized in October 1927 when the *Mathematics News*

Letter was published as Vol. 2, No. 1. By 1934 the journal had outgrown its regional roots so its name was changed accordingly to *National Mathematics Magazine*. However, the financial support that LSU provided from 1935 to 1942 was terminated when the state of Louisiana was forced by fiscal constraints due to World War II to slash the university's budget. To exacerbate the situation, the editor, S. T. Sanders, who had continually used his own funds to underwrite operational costs, reached mandatory retirement age at LSU that year. Deficits mounted alarmingly!

The MAA responded by providing subsidies but even those dried up in 1945, whereupon the *National Mathematics Magazine* abruptly ceased publication. Fortunately, one rabid reader, UCLA's Glenn James (1882–1961), developed a considerable empathy for Sanders and his journal, so he assumed sponsorship and management. Because the journal had grown to international dimensions, James shortened its title to the present MATHEMATICS MAGAZINE when he resumed publication in 1947. James, like Sanders, employed his whole family in every aspect of typesetting, printing, and mailing the journal. But by 1959 deteriorating eyesight caused him to negotiate with the MAA over the publication and editorship of the journal. The December 1960 issue revealed the complete transfer and the MAA has published it since then. We will see that four of the main characters in our group were involved with MATHEMATICS MAGAZINE in various ways before it became the second official journal of the MAA. (In 1974 the MAA initiated the *College Mathematics Journal*, which had been published by Prentice-Hall as the *Two-Year College Mathematics Journal* the previous four years.) Now we turn to our five main characters, examining their lives and works to see what roles these journals played in their development.

Farmer to founder

As we have noted, Joseph Benson Reynolds (1881–1975) is credited with the idea of forming the first MAA section in the East. Born in the western part of Pennsylvania, Reynolds did not graduate from high school until age 22 because he had to work on the family farm. A competitive scholarship allowed him to attend Lehigh, where he earned an A.B. degree in 1907 with an undergraduate thesis on temperature compensation of a sidereal clock, thus signaling an interest in applied mathematics. He then accepted an instructorship at Lehigh, where he spent the rest of his professional life. This was a typical appointment for those who desired to pursue graduate work because assistantships, as we know them today, did not arise until after World War II. Reynolds earned a master's degree in 1910 with a thesis on the orbit of a minor planet, a theme reflecting the genesis of Lehigh's Department of Mathematics and Astronomy. However, his doctoral dissertation, "The application of vector analysis to plane and space curves, surfaces and solids," submitted to Moravian College in 1919, reveals an evolving interest in pure mathematics. When he presented the first invited lecture at the organizational meeting of the Philadelphia Section in 1926, his topic paralleled the theme of the dissertation—evolutes of certain plane curves. He also served as chair of the section for 1938 and 1939.

Reynolds's publication record shows that the *Monthly* and this MAGAZINE provided vital outlets for many college teachers. His first formal entries were two proposed *Monthly* problems in 1915, one on calculus and the other on mechanics [**47**]. In the remainder of that year he solved three problems, with his solution to one posed by *Monthly* founder B. F. Finkel selected to appear in print [**48**]. The following year Reynolds proposed three other problems and solved one, but in the banner year 1917 he was cited 19 times—five proposed problems, three solutions to problems he had posed earlier, four printed solutions, and seven solutions listed under "also solved by."

Figure 1 Joseph B. Reynolds (Photograph courtesy of Lehigh University Archives)

His last proposed problem appeared in 1965 when he was 84 years old, exactly 50 years after his first [**49**].

The *Monthly* accounted for most of Reynolds's publication activity, with almost 200 entries appearing in connection with its problems department. Although there is sometimes a tendency among historians to criticize the orientation toward problems in early American mathematical journals, even the father of American mathematics, E. H. Moore, submitted solutions to six problems in *The Analyst* during his senior year at Yale. In fact, all five of our rank-and-file mathematicians submitted solutions to *Monthly* problems. The succession of Reynolds's other contributions traces his development as a mathematician. In his banner year 1917 he published a small note in the *Monthly* [**50**], but it would be six more years until his first full paper [**52**] would appear. His enduring interest in both pure and applied mathematics can be seen in a 1944 article that described a method for solving differential equations, where he claimed that his approach was appropriate for "every student who is trained for engineering or other scientific work" [**51**, p. 578]. In this respect Reynolds was somewhat ahead of his time, because shortly after World War II the country experienced a wave of teaching reforms aimed at satisfying the needs of the burgeoning number of students pursuing science and engineering in the nation's universities.

Joseph Reynolds published three papers in the MAGAZINE when it was called the *National Mathematics Magazine*. In 1938, he showed how to evaluate the integrals $\int \sin^n \theta \, d\theta$ and $\int \cos^n \theta \, d\theta$ for even integers n using Euler's forms for $\sin\theta$ and $\cos\theta$ [**45**], while in 1944 he presented geometrical interpretations of the formula for the statistical mean [**46**]. The third paper combined his interests in pure and applied mathematics by deriving an equation of an ellipse in order to explain the workings of a machine built by precision-tool manufacturers for cutting nuts (for bolts) in the shapes of various regular polygons [**53**]. A few other papers appeared in outlets like the *Mathematics Teacher*, the *Tôhoku Mathematical Journal*, and the *Proceedings of* *the Pennsylvania Academy of Science*, but Reynolds also published in several journals that reflect an overarching interest in applied mathematics, such as *Agricultural Engineering*, *Chemical and Metallurgical Engineering*, *Concrete*, *Automotive Industries*, *Iron Age*, and the *Journal of the American Welding Society*. It is worth noting that an item in *Science*, "Falling chimneys," corrected a result from a previous paper in that respected journal about where breaks in a chimney will occur (if at all).

Joseph Reynolds also wrote five textbooks, one a standard calculus book and the other four on theoretical mechanics. His *Elementary Mechanics* (1928) was revised six years after its initial publication and reprinted three years later. His proclivity toward applied mathematics might make him seem like an improbable candidate to found an MAA section, yet his interests paralleled those of many mathematicians around 1900, including several presidents of the AMS. He died in Sugar Run, Pennsylvania, at age 94. Overall he was a mathematician who carried out some original investigations and wrote several books but should be remembered mainly as a problemist. Moreover, his interest in astronomy, mechanics, and engineering hearken back to an earlier period in the history of mathematics in America. Reynolds had no apparent ties to the leading mathematical figures of the day, either during his student years or during his professional career, unlike our four remaining characters.

Blue-blooded founder

There is a stark contrast between Joseph Reynolds and Howard Hawks Mitchell (1885–1943). While Reynolds came from farming stock, Mitchell's father Oscar Howard Mitchell (1851–89) was the fifth person to obtain a doctorate (in 1882) from the country's first true graduate program at Johns Hopkins under the estimable J. J. Sylvester. And while Reynolds earned a Ph.D. at tiny Moravian at age 38, Mitchell was 26 when

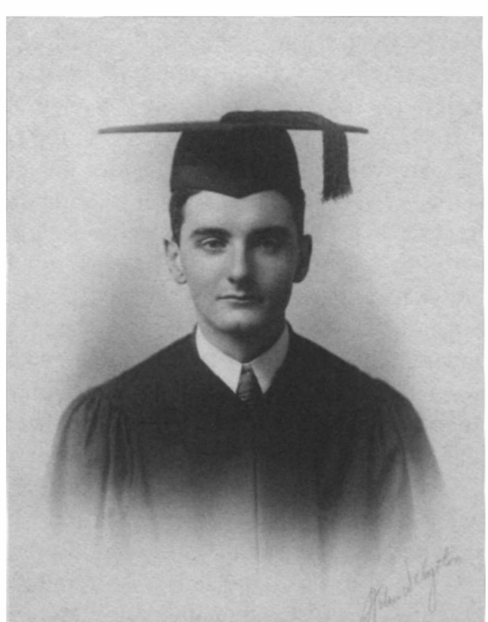


Figure 2 Howard Hawks Mitchell (Photograph courtesy of Special Collections, Dawes Memorial Library, Marietta College)

he received his doctorate at tony Princeton under Oswald Veblen. Yet he is virtually unknown today. FIGURE 2 shows Mitchell from the Marietta year book for 1906.

Howard Mitchell was born on January 14, 1885, in Marietta, Ohio. He graduated from Springfield (Massachusetts) High School before returning to his home town to attend Marietta College, where his father had been professor of mathematics and astronomy from 1882 until his untimely death. The son graduated from Marietta in 1906 as salutatorian with a Ph.B. degree. (No longer in use, Ph.B. is the abbreviation of the Latin term for Bachelor of Philosophy.) Mitchell then enrolled in the fledgling graduate program at Princeton, where he graduated in 1910 as Oswald Veblen's first official Ph.D. student. His dissertation was published in the *Transactions* one year later [**38**]. He was appointed an instructor at Yale University's Sheffield School in 1910, but the next year he accepted an instructorship at Penn, where he taught for the rest of his life. During his tenure Mitchell supervised five Ph.D. dissertations. (His most renowned student was probably Leonard Carlitz (1907–99), the number theorist who spent postdoctoral years at Cal Tech under E. T. Bell and at Cambridge under G. H. Hardy before settling at Duke 1932–77.) During World War I, Mitchell served as a ballistician under Oswald Veblen at Aberdeen Proving Ground; Grier [**26**] provides details on the type of work done there.

Howard Mitchell was the only member of our group whose involvement with the MAA was minimal. He did not even join the MAA before helping found the Philadelphia Section in 1926, and his membership afterwards was sporadic. But he remained active with the local section, serving as its first chair 1926–27 and again 1936–37, and delivering three one-hour invited lectures on quadratic forms (1926), group characters (1929), and Ramanujan (1932). Yet at the national level he held no elected offices, served on no committees, and edited no journals. However, he did serve a three-year term on the Board of Trustees of the AMS 1921–23, and a six-year stint as editor of the *Transactions* 1925–30. He was also elected vice president of the AMS 1932–33, and vice president and Chair of Section A of the American Association for the Advancement of Science in 1932. These positions suggest that Mitchell's major focus was on research mathematics and not undergraduate education.

We already noted a tie between the Mitchell family and Johns Hopkins, one of the two leading graduate programs in the country *circa* 1900. Studying under Veblen at Princeton linked Mitchell to the other program—the University of Chicago. And then in 1911, Mitchell was appointed an instructor at Penn at the same time as Chicago graduate R. L. Moore. Today Moore is widely known for his method of teaching and for his contributions to topology, but up to that point he had published very little. Yet Penn offered both instructors an especially supportive environment that allowed them to prosper. By the time Moore left for Texas in 1920, he had progressed from a promising mathematician to one of recognized stature, yet Mitchell was promoted sooner and produced a Ph.D. student earlier. On the other hand, Moore may have inspired Mitchell to teach the earliest known modified Moore Method course [**62**, p. 476].

Mitchell's publication record, though not prodigious, is impressive. For instance, in 1923 he co-authored an important book on algebraic numbers for the National Research Council with L. E. Dickson, H. S. Vandiver, and G. E. Wahlin. Between 1913 and 1918 he published seven important papers in his specialties of linear groups and algebraic number theory in the country's three research journals: two in the *American Journal*, one in the *Annals*, and four in the *Transactions*. Only two appeared after that. His 1926 article on ideals in quadratic fields was sandwiched between papers by two of the towering figures in American mathematics, Marshall Stone and Oswald Veblen [**40**]. Mitchell's final paper appeared in the *Monthly* in 1935 and harked back to his initial investigation on group theory and projective geometry [**39**]. It was his only MAA publication except for a solution to a *Monthly* problem [**41**]. He is the only member of our quintet never to contribute to the *National Mathematics Magazine*. Mitchell died of coronary thrombosis in 1943 at age 58.

Section promoter

While Joseph Reynolds wrote mainly for undergraduate-oriented publications and Howard Mitchell mainly for research journals, the remaining three members of our quintet contributed to both and participated equally in the MAA and the AMS. The first, Albert Arnold Bennett (1888–1971), like Mitchell a protégé of Veblen, was a colorful character who lived in the Philadelphia area on two separate occasions totaling only eight years. Bennett was born June 2, 1888, on the U.S. Reservation in Yokohama, Japan, where his parents were missionaries with the Rhode Island Baptist Association. At age 14 he came to Providence, RI, to live with relatives and complete his education. Since his father, two grandfathers, and many other family members were Brown graduates, he entered as a legacy applicant in 1906. After earning A.B. and A.M. degrees in 1910 and an Sc.M. in 1911, he entered the graduate program at Princeton, where he may have met Howard Mitchell because he later recalled, "H. H. Mitchell, whom I had known at Princeton, was, as always, generous and encouraging" [**A1**]. This accounts for Mitchell's recruitment into the effort to form a section of the MAA in Philadelphia 15 years later.

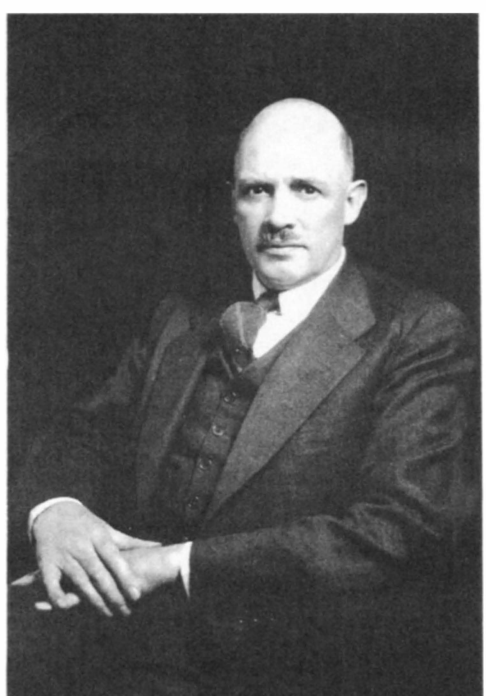


Figure 3 Albert A. Bennett (Photograph courtesy of Brown University Archives)

Like Mitchell, Bennett earned a Ph.D. under Oswald Veblen (in 1915) for a dissertation at the interface between algebra and projective geometry. It appeared in the *Annals* in 1915 [**4**]. Although only 21 pages long, it accounted for a sizable portion of the 196-page volume for 1914–15. That this neophyte would be accorded such recognition was probably due to the fact that three of the six editors were highly regarded faculty members at Princeton, where the journal was published: Veblen, Luther Eisenhart (1876–1965), and J. H. M. Wedderburn (1882–1948). Moreover, Bennett published three papers in the volume for 1916–17, all on topics in analysis, accounting for 47 of the journal's 217 pages.

Clearly Bennett's star was rising. He remained at Princeton as an instructor until the fall of 1916, when he accepted an adjunct professorship (what we would call today an assistant professorship) at the University of Texas. But patriotism compelled him to enroll in the Army's first Officer Training Corps (which evolved into today's R.O.T.C.) even though he was 28 years old at the time. In August 1917 Bennett was commissioned a captain in the artillery corps, C.A.R.C., and the following June was transferred to the Ordnance Department. He served on Veblen's ballistics research staff along with Gilbert Bliss, Norbert Wiener, and Howard Mitchell at Aberdeen Proving Ground, where he "prepared numerical methods to solve the ballistics equations" [**26**, p. 928]. Bennett was honorably discharged in January 1919, yet he served as a civilian mathematician and dynamics expert with the Ordnance Department until September 1921. During this time he wrote a book on ballistics that was initially classified "Confidential; for official use only" [**12**]; in 1954 the Ballistics Research Lab at Aberdeen deemed his tables important enough to warrant republication [**6**].

The time Bennett spent in war service undoubtedly accounts for a diminution in his publication record between 1917 and 1920. However, like many mathematicians caught up in war, he did not let combat duty extirpate his mathematical investigations. For instance, he is listed in a 1918 paper in the *Bulletin of the AMS* as Captain Albert A. Bennett, C.A.R.C. Emphasizing the isolation of his outpost he wrote, "This treatment is believed to be original, but the literature available for examination by the author is that customary to an army post, 'somewhere on the Gulf of Mexico,'—nil" [**5**, p. 479]. Apparently the holdings in Bennett's outpost were not as barren as one might infer from this statement. An examination of the *Monthly* reveals a different mathematical activity—problem solving—which can be pursued in short bursts of energy, unlike the sustained periods of intense mental concentration needed for deep research projects. From January 1917 to March 1918, Bennett was a regular contributor to the problems department, proposing seven and solving six others in algebra, number theory, and geometry. Curiously, the printed solution to one problem he proposed was by Joseph Reynolds, who would found the Philadelphia Section with Bennett almost ten years later [**16**]. A problem Bennett proposed in the September 1918 issue [**9**] lists his address as Galveston, thus identifying his whereabouts "somewhere on the Gulf of Mexico."

Bennett's problem-solving exploits ultimately placed him in "the ranks of those eminent in their chosen specialties who were impelled to contribute frequently ... while actively engaged in university teaching" [**58**, p. 8]. Joseph Reynolds too was cited with five "other problemists [who] upon becoming emeritus found continued problem-solving an effective weapon against vegetation." Both encomia appeared in the *Otto Dunkel Memorial Problem Book* [**25**], a special issue of the *Monthly* based upon the 400 best problems in the journal from 1918 to 1950. The selection panel singled out four problems Bennett had proposed, including an influential one he sent while at Texas in 1925 [**10**, p. 261]. Surprisingly he did not adopt the term semigroup in the problem, even though he had already used it in the title and abstract of a lecture at an annual AMS meeting [**11**, pp. 223–224]. The problem's classification under "Unsolved algebra problems" in the *Dunkel Book* [**25**, p. 68] sparked a solution the next year by the Polish problemist Andrzej Makowski [**35**]. Shorter solutions appeared in 1962 [**19**] and 1965 [**18**, p. 324] before the problem was finally laid to rest [**60**, pp. 915–916].

In the fall of 1921, his war duties completed, Bennett resumed his career at Texas. One of his first activities was to found an undergraduate mathematics club, The Pentagram, which played a minor role in the evolution of the Moore Method [**62**, p. 477]. Bennett had been active with the Maryland-Virginia-DC Section of the MAA while stationed at Aberdeen, and he extended those endeavors to the national level upon reaching Texas, being elected a trustee, appointed to the Committee on Publications, and appointed editor-in-chief of the *Monthly*. He was elected vice-president of the MAA in 1925 (and again in 1933 and 1934) while at the same time chairing its Texas Section. He had to forego the latter position when he became professor and head of the department at Lehigh, a post he held for only two years before returning to Brown, his *alma mater*. It was during Bennett's two years at Lehigh that he was the main cog in founding the Philadelphia Section after being "urged to wake up some sectional activity" [**A1**]. Upon moving to Brown, Bennett's attempt to form a New England Section of the MAA was unsuccessful, mainly because the Association of Teachers of Mathematics in New England (ATMNE) was then in the hands of college professors from the Boston area. In fact, Bennett was elected president of the ATMNE in 1941. However, by 1955 college teachers felt the need for an MAA section so Bennett served as temporary chair at an organizational meeting arranged by Howard Eves, Donald Kearns, and John Kemeny to found the Northeastern Section. A history of that section aptly described Bennett as "an experienced section promoter" [**42**, pp. 101–102].

The moves from Austin to Bethlehem to Providence had little effect on Bennett's production of research articles, although his publication record at Lehigh was modest. Perhaps his best-known works are a book on formal logic [**15**] he coauthored with Charles A. Baylis (1902–75) and his brief history of the MAA up to World War II [**8**]. Of more relevance here is Bennett's growing involvement with educational issues. Beginning in the early 1920s he wrote a host of articles on pedagogy and the curriculum. In 1927 he was appointed chair of the MAA's Committee on Assigned Collateral Readings in Mathematics, which drew up a list of suggested assignments for a freshman-year course based on outside reading [**36**, p. 30], and from 1941 to 1945 he served as chair of the MAA's Conference Committee on Education. In between he published an article in the *Monthly* on teacher training based on an invited address delivered at the 1938 joint MAA meeting with the National Council of Teachers of Mathematics. Bennett was assigned the topic of methodology but he protested, "Common decency suggests that the college professor either make a careful study of the problem of teacher preparation or refrain from making judgment" [**13**, p. 214]. Yet he moved quickly beyond common decency, adding a steady flow of "ungracious words" on issues related to teacher preparation, such as whether mathematics departments should offer courses in methodology and what courses should be required of future high-school teachers. His unsparing criticism of the behavior of some professors became enmeshed with a veiled attack on the central role of research in universities: "Some professors have atrocious table manners, or are extremely slovenly as to dress, or succeed very poorly in transmitting and evoking ideas in the classroom. But such disagreeable details are often condoned in the presence of more valued attributes" [**13**, p. 216].

Bennett continued railing against the prevailing preparation of high-school teachers in an article published in this MAGAZINE. He expressed a fear that enrollments in mathematics courses during World War II would decline precipitously once wartime programs ended, but, as we now know, that never occurred. However, his thoughts on various ways to present mathematics in an attractive manner remain relevant today. The article concluded, "If its practical utility, its beauty, its essential role in interpreting the times becomes clear... no one need fear for the mathematical education of the next generation" [**14**, p. 322].

The patriotic Bennett rejoined the Army at age 54 when World War II broke out, serving from 1942 to 1946 and being promoted from Major to Lieutenant Colonel.

Once again he was assigned to the Ordnance Department at Aberdeen under Oswald Veblen. After the war, he was sent to the country of his birth to survey Japanese weaponry. One of the more illustrious young mathematicians to work at Aberdeen under Bennett was Herman Goldstine (1913–2004), who, in a 1985 interview, described his boss in most ungracious terms: "From time to time I was very impatient of Albert Bennett, who was a nice old gentleman—but he was a very precise, methodical, plodding person who drove me up the wall" [**59**].

Bennett retired from Brown in 1958 but subsequently taught at three other colleges. His devotion to teaching remained strong to the end. An obituary revealed that he "taught last week, but called BC [Boston College] early this week, saying he had the flu and wouldn't be in until next Thursday" [**A2**]. He died that Wednesday evening in 1971 at age 82, having been a member of the MAA for all of its 55 years. In his address on teacher training, he cited one textbook as a model for presenting the appropriate spirit of mathematics. One of the authors of that book was J. R. Kline, who, for reasons we explain below, was *not* one of the founders of the Philadelphia Section.

Moore-trained leader

John Robert Kline (1891–1955) was arguably the most influential mathematician in Philadelphia from 1920 to 1950. He should be much better known for, among other things, his support of African-Americans at a time when such encouragement was not the norm. Born December 7, 1891, in Quakertown, near Philadelphia, J. R. Kline obtained an A.B. in 1912 from Muhlenberg College (located in nearby Bethlehem) and a year later enrolled in the graduate program at Penn, where two newly hired instructors were Howard Mitchell and R. L. Moore. Apparently Kline took two courses with Moore: Foundations of Mathematics, and a sequel called Theory of Point Sets. Beyond these, individual study was the fashion, with Moore encouraging his better students to work solely with him. Kline thrived under the Moore Method, obtaining a master's degree in 1914 and a Ph.D. two years later for a dissertation that was completed in 1915 and published in the *Annals* the next year [**30**].

After teaching at Muhlenberg 1915–16, Kline accepted an instructorship at Penn so he could continue to work with Moore. He left Penn in 1918 but returned two years later (after one year at Yale and another at the University of Illinois) to replace Moore, who had moved to Texas. Although Moore remained at Texas and Kline at Penn for the rest of their lives, the archives at the Center for American History in Austin contain a steady stream of correspondence between the two. Moreover, each sent students to study under the other, either during their graduate studies or as post doctorates. Kline took several leaves of absence from Penn, including a one-year stay 1926–27 as a Guggenheim Fellow in Göttingen, which explains why he was *not* a founder of the Philadelphia Section. However, he played an active role thereafter, being elected secretary-treasurer 1927–28 and chair 1932–33. At Penn he served as chair from 1940 until his untimely death in 1955.

During his tenure, Kline directed nineteen doctoral dissertations. His first student, Harry M. Gehman (1898–1981; Ph.D. 1925), served the MAA as secretary-treasurer 1948–60 and, when that position was bisected, as treasurer 1960–67. Kline was a particularly fair and unbiased man who permitted any qualified candidate to study under him. Two cases are particularly noteworthy. In 1928, he supervised the doctoral dissertation of Dudley W. Woodard, who became the second African-American student to receive a Ph.D. in mathematics in the United States. William Claytor became the third when he completed his dissertation in 1933. (The first, Elbert Cox, received his degree at Cornell University in 1925 [**20**].)

J. R. Kline became a respected member of the international mathematical community, publishing four papers in the Polish journal *Fundamenta Mathematicae* and three in the *Proceedings of the National Academy of Science*. Moreover, he wrote a joint paper with his advisor, the only publication Moore ever coauthored [**43**]. (This is not particularly surprising in light of the extreme individual competitiveness that underlies the Moore Method.) Most of Kline's publications appeared from the time of his dissertation in 1916 to a long paper on separation axioms in topology in 1928 [**32**].

Figure 4 J. R. Kline (Photograph courtesy of the American Mathematical Society)

Kline and two of his students lent active support to the MAGAZINE. As secretary of the AMS during 1941–42, he wrote strong letters urging officials in Louisiana to restore the journal's subsidy, which had been slashed from \$2700 to \$600. He also supplied the names and addresses of 5000 mathematicians to be sent a circular describing the journal and inviting subscriptions. These actions led to his inclusion among ten prominent figures cited in a note titled "Noblesse oblige!" [**55**]. In 1943, Norman Ely Rutt (1900–91) contributed "A peak individual donation!" of \$50 to the journal [**56**]. Rutt received his 1928 Ph.D. under Kline, spent two postdoctoral years at Texas with R. L. Moore, taught at LSU 1936–66, and contributed actively to the MAGAZINE. The other Kline student, MAA secretary-treasurer Harry Gehman, informed Glenn James in 1959 that the MAA had agreed to take over full management.

J. R. Kline became very concerned with graduate education, as witnessed by his final paper, which sheds light on the state of mathematics in the country after World War II. In late November 1945, six months after VE Day, he presented his views on rebuilding graduate departments in an address at the annual MAA meeting. His remarks were published the following March under the title, "Rehabilitation of graduate work" [**31**]. Kline felt strongly that the steep decline in the production of mathematics Ph.D.s from 104 in 1941 to 39 in 1944 had to be reversed by invigorating the country's graduate programs. He noted the deleterious effects of the Draft Board, which granted no deferments for mathematicians and graduate students until July 1942, and then only for those teaching at least 15 hours per week. Yet even that deferment was abolished within two years. Because of this, at the end of the war the country found itself with only 1675 Ph.D.s in mathematics among 4600 college teachers at the rank of instructor or above. Moreover, due to the GI Bill, mathematics enrollments in the fall of 1945 tripled. Kline cited some egregious conditions he felt must be changed, like frozen salaries and high teaching loads. He also emphasized the need to "re-condition" researchers about to resume academic careers. In conclusion, he proposed two immediate initiatives: preferential demobilization, and the establishment of a system of fellowships for postdoctoral students (like those the National Research Council formerly administered), full-time graduate students, and superior undergraduates. Although the first initiative never materialized, the second exceeded even Kline's expectations when the National Science Foundation was established in 1950. Unfortunately, a prolonged and progressive illness led J. R. Kline to commit suicide in May 1955 at age 63.

Twelve years earlier, Kline had served on the joint AMS-MAA Committee on Available Teachers in Collegiate Mathematics. Established by the War Policy Committee, its charge was to compile and maintain a register of vacancies and availability of mathematicians for service throughout the war. Arnold Dresden, a neighbor of Kline's, was one of the two other members. In the early 1930s this duo took part in an exchange between Penn and two area colleges that sent Kline, Howard Mitchell, and Hans Rademacher to teach at Swarthmore and Bryn Mawr while Dresden and Heinrich W. Brinkmann (from Swarthmore) and Anna Pell-Wheeler and Gustav A. Hedlund (from Bryn Mawr) proceeded inversely.

Music lover, Santa looker

Arnold Dresden (1882–1954) was a native of Amsterdam who attended the university there for three years. However, in 1903, and against his parents' wishes, he used tuition money to book passage to New York in order to help a friend in Chicago, where he arrived on November 23, his twenty-first birthday. During his first two years in the Windy City, Dresden worked at various jobs, including stacking merchandise at the Marshall Fields wholesale warehouse at $10 a week. He also taught six classes at the high school associated with the University of Chicago called the Laboratory School, a task he faced with grave misgivings because, as he recalled, "In Holland we tortured our teachers" [**1**, p. 5], but he had no trouble maintaining discipline in America.

By 1905, Dresden had scraped together enough money to enroll at the University of Chicago. He received his Ph.D. four years later, writing a dissertation on the calculus of variations under Oskar Bolza. Then he accepted an assistant professorship at the University of Wisconsin, where he remained for eighteen years. A naturalized citizen since 1913, Dresden's humanitarian bent compelled him to participate in World War I by working for the Red Cross in France during 1918–19.

The May 1927 *Monthly* heralded his arrival in the Philadelphia area nine months after the MAA section was founded: "Professor Arnold Dresden of the University of Wisconsin has been appointed professor of mathematics at Swarthmore College. An interesting feature of his work in that college will be in connection with the honors course for juniors and seniors" [**33**, p. 277]. Dresden described this course in a 1931 lecture to the Philadelphia Section of the MAA. Minutes from that meeting record only that he gave "an account of the way in which this plan [for honors work] is realized, particularly in mathematics and the natural sciences" [**17**]. Fortunately the *Monthly* supplied more details [**33**, p. 277]:

> Students in that course are not obliged to attend classes, are free to work at tasks assigned to them on which they have conferences with their instructors as often as may seem desirable. No grades or records are kept during these two years.

> At the end of the senior year they have to take a comprehensive examination covering the work of these two years and conducted both in oral and written parts by an outsider.

The honors program that Dresden designed required students to complete four seminars in mathematics and two in each of two minors, which constituted the student's whole course load during the final two years. External examiners conducted all assessment. Although parts of the system have been drastically revised, external examiners remain an integral part of the program today.

Arnold Dresden became one of the most respected and effective leaders in both the AMS and the MAA. At the second meeting of the fledgling Philadelphia Section in November 1927, he presented an invited lecture, "On matrix equations," reporting on a method (to determine solutions of polynomial matrix equations in which the constant term is missing) that had just been developed by his only Ph.D. student, William Edward Roth. Dresden was promptly elected to the Program Committee; he would be elected again in 1939. He was also elected chair for two two-year terms, 1931–32 and 1940–41. During his first summer in the East (1928) he taught courses at Penn with both Kline and Mitchell.

Dresden began his publishing career in 1907 while still a graduate student at Chicago, writing two papers on the calculus of variations. Part of his dissertation appeared in the *Transactions* the following year [**23**]; further advances appeared in 1916, 1917, and 1923. In 1923 he also published two papers on symmetric forms in n variables. But from that time on, with only a few exceptions, all submissions seem to have been restricted to the MAGAZINE and the *Monthly*.

Dresden was an early, ardent advocate of the MAA. In 1915, he sent a strong letter of support for the idea of forming the Association to Herbert Slaught, who was trying to gauge the degree of backing for the idea that took root at the end of the year. However, it was not until Dresden's move to Swarthmore that his focus changed from the AMS to the MAA. He was elected president for 1933 (succeeding E. T. Bell; Albert Bennett was vice-president) after having served as vice president for 1931.

Two noteworthy events occurred during Dresden's presidency. One took place on a tour of the South over his Easter vacation, when he presented two lectures at the joint meeting of the Louisiana-Mississippi sections of the MAA and NCTM. The section chair exhorted the membership to "give him a hearty welcome into the splendid fellowship of our sections" [**57**, p. 96], resulting in a throng of eighty-five people attending his address at the banquet on Friday night, "The Mathematical Association of America and American mathematics," and his lecture on Saturday morning, "Some aspects of the calculus of variations." The report of the meeting cited his willingness to participate: "Besides bringing us very helpful addresses Prof. Dresden frequently entered the discussions which were unusually fine at these meetings" [**37**, p. 82].

Arnold Dresden's retiring MAA presidential address for 1934, "A program for mathematics," published in the *Monthly* the following April, encapsulated his deep concern about the place of mathematics in general culture and about the mathematical community's laissez-faire attitude toward the role it should play. He wrote, "It is my firm conviction that both the content and the spirit of mathematics have a great deal to contribute to the education of the individual" [**21**, p. 200]. A recurring theme was his belief that abstract concepts can be grasped by young people, which he preached in his 1936 book, *An Invitation to Mathematics* [**22**]. Although ostensibly intended for a liberal arts audience, the contents include the number system, point set theory, types of infinity, foundations of geometry, noneuclidean geometry, analytic geometry, projective geometry, calculus, differential equations, vector analysis, and the theory of numbers. A review in the *Monthly* [**34**] opined that due to Dresden's original approach, "incredible as it may appear, 'the preparation that is indispensable for the use of this book does not exceed what is furnished by a good high school course in algebra and in plane geometry'." In another review, the sometimes truculent Albert Bennett raved, "The book is the outcome of several years of classroom experience... the reader may hope to find not only much of the charm and symmetry of mathematics but as well a lively appreciation of the fundamental significance for the modern life of the expanding achievements of mathematical science" [**7**, p. 535]. This enthusiasm was shared by Texas mathematician H. J. Ettlinger, who concluded, "There is every reason to commend the author for a real contribution to American mathematical text books" [**24**, p. 289]. Judging by the lack of advertising for this book after its initial run, it appears that financial success did not follow critical acclaim.

Dresden's other textbook, *Introduction to Calculus* (1940), which aimed to provide a rigorous approach (for instance, introducing Dedekind cuts to develop the real line) did not even receive critical commendation. A review by Alston Scott Householder (1904–93), famous today for his eponymous transformations in linear algebra, expressed reservations about the ability of American sophomores to handle this level of rigor, yet he looked forward to adopting it, adding, "It will be a distinct pleasure to try out this book in the class" [**27**, p. 50]. However, two years later Householder admitted, "The purpose is admirable, but it is hard to see how justice can be done to Dresden's text in eight semester hours with any but a very exceptional class" [**28**, p. 45].

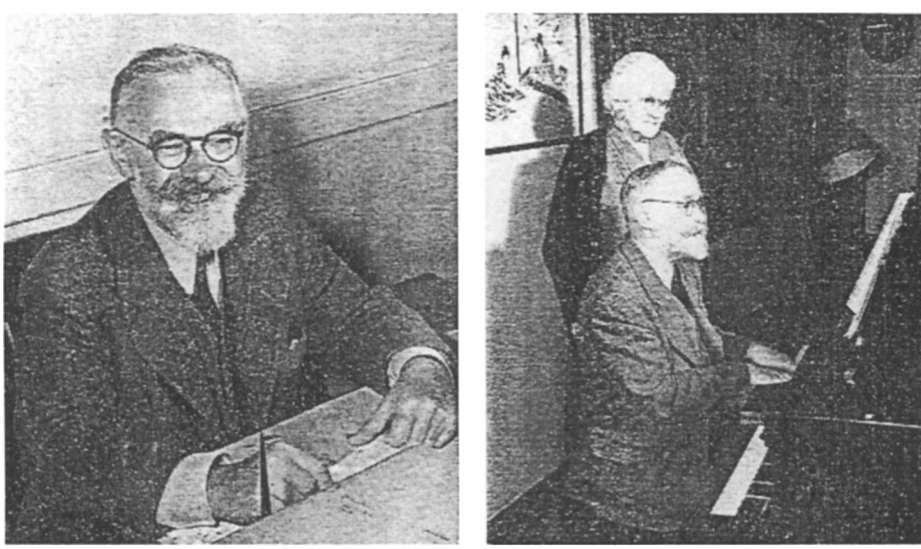


Figure 5 Arnold Dresden (Photographs courtesy of the Friends Historical Library of Swarthmore College)

At Swarthmore, as at Wisconsin, Dresden was known as much for his wide interests and musical talent (especially the piano) as for his mathematics, and his Monday evening chamber music sessions were celebrated. Students adored him. The alumni magazine gushed, "Of all the people on Swarthmore's faculty, one of the most beloved is a man who could easily be mistaken for Santa Claus, both in spirit and in the flesh" [**1**, p. 5]. When asked about the history of his beard, called "the finest hirsute adornment on campus," he replied, "Why, I've had it ever since I was born" [**1**, p. 10]. Arnold Dresden resided in the town of Swarthmore from the time of his appointment in 1927 until his death in 1954 at age 71. He had retired from active teaching just two years earlier, ably succeeded by David Rosen (1921–2003), who continued his role with the honors program and active participation with the MAA [**61**, p. 119].

Summary

We have described the lives and work of five leaders of the Philadelphia Section of the MAA who prospered in the second quarter of the twentieth century. The three founders (Joseph Reynolds, Howard Mitchell, and Albert Bennett) and two early leaders (J. R. Kline and Arnold Dresden) were local maxima but globally operated in the shadows of giants, like E. H. Moore, Oswald Veblen, and R. L. Moore. Table 1 shows that our five were born in one eleven-year period and received their doctorates in another.

TABLE 1: The five at a glance

	Birth	Death	Ph.D.	Institution	Supervisor
Reynolds	1881	1975	1919	Moravian	N/A
Mitchell	1885	1943	1910	Princeton	Veblen
Bennett	1888	1971	1915	Princeton	Veblen
Kline	1891	1955	1916	Pennsylvania	R. L. Moore
Dresden	1882	1954	1909	Chicago	Bolza

The three founders were quite different. Reynolds was interested in applications of mathematics to astronomy, mechanics, and engineering. Mitchell was a specialist in group theory. Bennett switched from being primarily a researcher to an administrator with a strong interest in educational issues, particularly teacher training. Kline and Dresden were alike. They lived in the same small town and developed deep concerns for the state of mathematics education in America, Kline at the graduate level and Dresden the undergraduate. Dresden designed a program for honors students at Swarthmore College that served as a model for highly selective, small, liberal arts colleges. Kline suggested initiatives for rehabilitating graduate education after World War II that were realized shortly with the advent of the National Science Foundation.

Reynolds had no direct ties to national leaders but the other four had links to the Chicago school initiated by E. H. Moore in 1892. Just look at their Ph.D. supervisors in Table 1—Oswald Veblen and R. L. Moore were prize graduates of E. H. Moore himself, while Oskar Bolza was the first professor hired by E. H. Moore. Mitchell was Oswald Veblen's first Ph.D. student at Princeton, Bennett his fourth, and both worked with Veblen at Aberdeen during WWI. (Bennett also served under Veblen during WWII; Mitchell was critically ill at the time.) Moreover, Kline played a pivotal role in the genesis of the Moore Method, and Dresden's program at Swarthmore was undoubtedly influenced by the teaching philosophy of E. H. Moore.

No professional organization can survive without a significant community of rank-and-file enthusiasts who are receptive to the work of the leaders and who are able and willing to participate in all aspects. Our quintet played this role, standing on the lower rungs of the AMS ladder but ascending to the upper ranks of MAA leadership and contributing to its official journals—this MAGAZINE and the *Monthly*. When the MAA was founded in late 1915, Reynolds was 34 years old, Dresden 33, Mitchell 30, Bennett 27, and Kline 24. All five were young faculty members (at Lehigh, Wisconsin, Penn, Princeton, and Muhlenberg, respectively), yet only Reynolds, Dresden, and Bennett became charter members of the fledgling Association. Kline would join the next year after returning to Penn to be with R. L. Moore, another charter member. However, it would be another 10 years before Mitchell would join. While Mitchell's membership in the MAA lapsed, the other four held theirs until the end of their lives.

Locally, our quintet sparkled on the top rung of the Philadelphia Section ladder. The American mathematical community benefited greatly from their efforts and they deserve to be rescued from their present obscurity.

REFERENCES

Archival Sources

A1. Albert A. Bennett to Voris V. Latshaw, 27 December 1967, EPADEL Archives, Special Collections, Temple University Libraries, Philadelphia, PA.

A2. Newspaper clipping, "Dr. A. A. Bennett dies; Was Brown professor," *The Providence Journal*, February 18, 1971, Archives, The John Hay Library, Brown University.

Published Sources

1. Anon, Dresden: Mathematics and the man, *The Garnet Letter*, February 1950, pp. 5, 10.
2. R. C. Archibald, *A Semicentennial History of the American Mathematical Society, Vol. I, History*, American Mathematical Society, New York, 1938.
3. E. F. Beckenbach, *Mathematics Magazine*: The first half century, this MAGAZINE **50** (1977), vii–xxvi.
4. A. A. Bennett, An algebraic treatment of the theorem of closure, *Annals Math.* **16** (1914–1915), 97–118.
5. ———, An elementary derivation of the probability function, *Bull. AMS* **24** (1918), 477–479.
6. ———, *Bennett Tables for Interior Ballistics by the Method of Albert A. Bennett*, Ballistics Research Laboratory, Aberdeen, MD, 1954.
7. ———, Book review, *Science* **84** (1936), 535.
8. ———, Brief history of the Mathematical Association of America before World War II, *Amer. Math. Monthly* **74** (1967), Part II: Fiftieth Anniversary Issue, 1–11.
9. ———, Problems and solutions, *Amer. Math. Monthly* **25** (1918), 302.
10. ———, Problems and solutions, *Amer. Math. Monthly* **32** (1925), 261.
11. ———, Semi-groups, *Bull. AMS* **31** (1925), 223–224.
12. ———, *Tables for Interior Ballistics*, Government Printing Office, Washington, DC, 1923.

→ ———, The college teacher of mathematics looks at teacher training, *Amer. Math. Monthly* **46** (1939), 213–224.

14. ———, Trends in the teaching of secondary school mathematics, *National Math. Mag.* **18** (1944), 315–322.
15. ——— and C. A. Baylis, *Formal Logic: A Modern Introduction*, Prentice-Hall, New York, 1939.
16. ——— and J. B. Reynolds, Problems and solutions, *Amer. Math. Monthly* **24** (1917), 469.
17. P. A. Caris, The sixth annual meeting of the Philadelphia Section, *Amer. Math. Monthly* **39** (1932), 61–62.
18. W. E. Coppage, Solutions of advanced problems, *Amer. Math. Monthly* **72** (1965), 324.
19. T. M. K. Davison, Advanced problems and solutions, *Amer. Math. Monthly* **69** (1962), 237–238.

→ J. A. Donaldson and R. J. Fleming, Elbert F. Cox: An early pioneer, *Amer. Math. Monthly* **107** (2000), 105–128.

→ A. Dresden, A program for mathematics, *Amer. Math. Monthly* **42** (1935), 198–208.

22. ———, *An Invitation to Mathematics*, Henry Holt & Co., New York, 1936.

→ ———, The second derivatives of the extremal-integral, *Trans. AMS* **9** (1908), 467–486.

→ H. J. Ettlinger, Book review, *National Math. Mag.* **11** (1937), 288–289.

25. H. Eves and E. P. Starke, eds., *The Otto Dunkel Memorial Problem Book*, *Amer. Math. Monthly* **64** (No. 7, Part 2), Mathematical Association of America, Menasha, WI, 1957.

→ D. A. Grier, Dr. Veblen takes a uniform: Mathematics in the First World War, *Amer. Math. Monthly* **108** (2001), 922–931.

→ A. S. Householder, Book review, *National Math. Mag.* **15** (1940), 49–50.

28. ———, Book review, *National Math. Mag.* **17** (1942), 45.
29. P. S. Jones, Historical background and founding of the Association, in [**36**], pp. 1–23.
30. J. R. Kline, Double elliptic geometry in terms of point and order, *Annals Math.* **18** (1916), 31–44.

→ ———, Rehabilitation of graduate work, *Amer. Math. Monthly* **53** (1946), 121–131.

32. ———, Separation theorems and their relations to recent developments in analysis situs, *Bull. AMS* **34** (1928), 155–192.
33. H. W. Kuhn, ed., Notes and news, *Amer. Math. Monthly* **34** (1927), 275–280.
34. H. F. Mac Neish, Reviews, *Amer. Math. Monthly* **44** (1937), 324.
35. A. Makowski, Advanced problems and solutions, *Amer. Math. Monthly* **65** (1958), 371.
36. K. O. May, ed., *The Mathematical Association of America: Its First Fifty Years*, Mathematical Association of America, Washington, DC, 1972.

37. D. McCoy, The Louisiana-Mississippi Section of the MAA and NCTM, *National Math. Mag.* **9** (1934), 82–84.
38. H. H. Mitchell, Determination of the ordinary and modular ternary linear groups, *Trans. AMS* **12** (1911), 207–242.
39. ———, Linear groups and finite geometries, *Amer. Math. Monthly* **42** (1935), 295–297.
40. ———, On classes of ideals in a quadratic field, *Annals Math.* **27** (1926), 297–314.
41. ———, Problems and solutions, *Amer. Math. Monthly* **38** (1931), 295–297.
42. H. F. Montague, The sections, in [**36**], pp. 78–103.
43. R. L. Moore and J. R. Kline, On the most general plane closed point-set through which it is possible to pass a simple continuous arc, *Annals Math.* **20** (1919), 218–223.
44. K. H. Parshall and D. E. Rowe, *The Emergence of the American Mathematical Research Community, 1875–1900: J. J. Sylvester, Felix Klein, and E. H. Moore*, American Mathematical Society, Providence, RI, 1994.
45. J. B. Reynolds, On Euler's forms, *National Math. Mag.* **12** (1938), 294–295.
46. ———, On interpreting a formula, *National Math. Mag.* **19** (1944), 37–39.
47. ———, Problems and solutions, *Amer. Math. Monthly* **22** (1915), 61–62.
48. ———, Problems and solutions, *Amer. Math. Monthly* **22** (1915), 319.
49. ———, Problems and solutions, *Amer. Math. Monthly* **72** (1965), 548.
50. ———, Relating to a curve with unusual properties, *Amer. Math. Monthly* **24** (1917), 343–344.
51. ———, Reversion of series with applications, *Amer. Math. Monthly* **51** (1944), 578–580.
52. ———, The area of ruled surfaces by vectors, *Amer. Math. Monthly* **30** (1923), 185–189.
53. ———, The mathematics of a nut cutter, *National Math. Mag.* **19** (1945), 159–162.
54. N. E. Rutt, Book review, *National Math. Mag.* **17** (1942), 92–93.
55. S. T. Sanders, Noblesse oblige! *National Math. Mag.* **16** (1942), 170.
56. ———, A peak individual donation! *National Math. Mag.* **18** (1944), 152.
57. P. K. Smith, Louisiana-Mississippi section and council programs, *Mathematics News Letter* **8** (1934), 96.
58. C. W. Trigg, The *Monthly* problem departments, 1894–1954, in [**25**], pp. 3–8.
59. A. Tucker and F. Nebeker, An interview with Herman Goldstine, in *The Princeton Mathematics Community in the 1930s*, Transcript Number 15, Princeton University, 1985.
60. A. Wilansky, Solutions of advanced problems, *Amer. Math. Monthly* **72** (1965), 915–916.
61. D. E. Zitarelli, *EPADEL: A Semisesquicentennial History, 1926–2000*, Raymond-Reese Book Co., Elkins Park, PA, 2001.
62. ———, The origin and early impact of the Moore Method, *Amer. Math. Monthly* **111** (2004), 465–486.
63. ———, Towering figures of American mathematics, 1890–1950, *Amer. Math. Monthly* **108** (2001), 606–635.

In De Morgan's Grocery

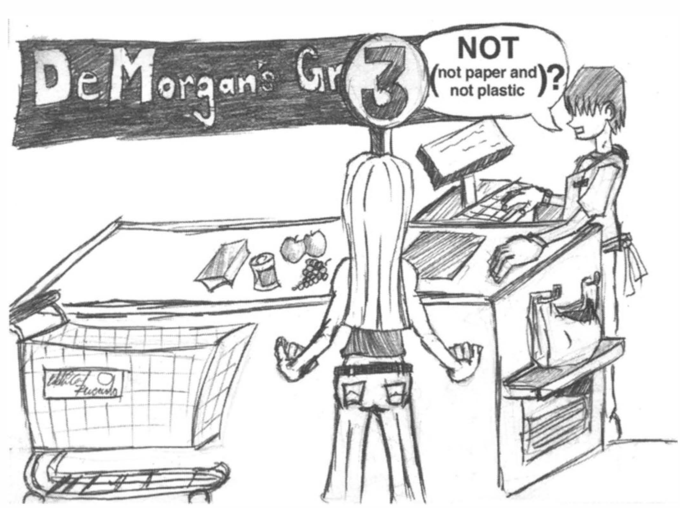


image by Amy Schumer and Eddingel Recaido

—PETER D. SCHUMER
MIDDLEBURY COLLEGE
MIDDLEBURY, VT 05753

Farmer Ted Goes 3D

SHAWN ALSPAUGH
Indiana University
Bloomington, IN 47405
shalspau@indiana.edu

In his recent paper entitled "Farmer Ted Goes Natural" [2], Greg Martin discusses the plight of Farmer Ted, who wants to minimize the cost of chicken wire to enclose a rectangular coop with a base of 190 square feet. However, Farmer Ted has difficulty purchasing $4\sqrt{190}$ feet of chicken wire because he is only able to purchase wire in integer lengths. After much deliberation, he decides to build an 11 foot $\times$ 17 foot coop (187 square feet), which has the best cost-efficiency of any possible coop with integer side lengths and area 190 square feet.

Here we add another dimension to the story of Farmer Ted. In recent years, Farmer Ted has helped numerous neighbors efficiently build chicken coops. Then one local farmer asked a question that intrigued him: The farmer wants to build an animal cage with a volume of up to 50 cubic feet. What is the most cost-effective way to do this with integer side lengths?

Farmer Ted had begun to think in 3D.

Before analyzing the three-dimensional problem, we should briefly review some of Martin's work. He starts with the basic calculus optimization problem of finding the minimum perimeter of a rectangle given a fixed area. As many students know, the optimal shape is a square. Martin then offers this variation: Given a positive integer N, what are the dimensions of the rectangle with *integer side lengths* and area at most N whose area-to-perimeter ratio is largest among all such rectangles?

In order to solve this problem, Martin makes the following definitions: Let $s(n) = \min(c + d)$ where $cd = n$ and $c, d \in \mathbb{N}$. Equivalently, $s(n) = \min(d + n/d)$ where $d \mid n$. This gives the minimum semiperimeter, or half of the actual perimeter, of a rectangle with area n with integer sides. Define $F(n) = n/s(n)$, which is the maximum ratio of area to semiperimeter for a given n. (Using this expression, which is twice as large as the maximum ratio of area to perimeter, is more aesthetically pleasing and does not change the analysis.) Farmer Ted prefers to enclose 187 ft.^{2} rather than 190 ft.^{2} because $F(187) = 187/28 > F(190) = 190/29$.

This leads Martin to identify the set

$$\mathcal{A} = \left\{n \in \mathbb{N} : F(k) \le F(n) \quad \text{for all} \quad k \le n\right\},$$

which lists the areas of integer rectangles such that no rectangle with smaller area has a greater area-to-semiperimeter ratio. By brute force, we can see that the first 59 elements of $\mathcal{A}$ are

$$\begin{aligned}\mathcal{A} = \{&1, 2, 3, 4, 6, 8, 9, 12, 15, 16, 18, 20, 24, 25, 28, 30, 35, 36, 40, 42, 48, 49, 54,\\ &56, 60, 63, 64, 70, 72, 77, 80, 81, 88, 90, 96, 99, 100, 108, 110, 117, 120, 121,\\ &130, 132, 140, 143, 144, 150, 154, 156, 165, 168, 169, 176, 180, 182, 192, 195,\\ &196, \ldots\}.\end{aligned}$$

Every square integer belongs to $\mathcal{A}$; after all, the original calculus problem leads Farmer Ted to a square pen. Martin coined the term *almost-squares* for the elements of $\mathcal{A}$. His main theorem allows us to enumerate the almost-squares.

THEOREM 1. (MARTIN) *For any integer $m \geq 2$, the set of almost-squares between $(m-1)^2+1$ and m^2 (inclusive) consists of two flocks, the first of which is*

$$\{(m+a_m)(m-a_m-1), (m+a_m-1)(m-a_m), \ldots, (m+1)(m-2), m(m-1)\},$$

where

$$a_m = \left\lfloor \frac{\sqrt{2m-1}-1}{2} \right\rfloor,$$

and the second of which is

$$\{(m+b_m)(m-b_m), (m+b_m-1)(m-b_m+1), \ldots, (m+1)(m-1), m^2\},$$

where

$$b_m = \left\lfloor \sqrt{\frac{m}{2}} \right\rfloor.$$

The reader can observe the flocks between pairs of squares in our list. Martin's first corollary gives another, more interesting characterization of the almost-squares involving triangular numbers. These are numbers of the form $t_n = \binom{n}{2} = n(n-1)/2$. Defining $T(x)$ as the number of triangular numbers not exceeding x, we can state his first corollary.

COROLLARY 1. (MARTIN) *The almost-squares are precisely those integers that can be written in the form $k(k+h)$, for some integers $k \geq 1$ and $0 \leq h \leq T(k)$.*

Martin also produced a polynomial that asymptotically counts almost-squares and showed the existence of polynomial-time algorithms for many processes.

The next dimension

Now let us extend Martin's results into a third dimension. We pose the following problem: given a positive integer N, find the dimensions of the rectangular box with (positive) integer sides and volume at most N whose volume-to-surface-area ratio is largest among all such rectangular boxes. The other possible formulation would be to compare the volume of the box to the sum of the side lengths; we study the former, as it seems the more natural extension to consider.

To begin, we must redefine some of the terms Martin used. As before, without changing the analysis, we work with semi-surface area, or half the actual surface area, to avoid repeatedly dividing by 2. First, we will define the minimum possible semi-surface area of a box of volume n to be

$$s(n) = \min(xy + yz + xz), \qquad \text{where} \quad xyz = n \quad \text{and} \quad x, y, z \in \mathbb{N},$$

or equivalently

$$s(n) = \min(xy + n/x + n/y), \qquad \text{where} \quad x, y \in \mathbb{N} \quad \text{and} \quad x \mid n,\ y \mid n.$$

Let $F(n) = n/s(n)$ denote the ratio of volume to the minimum semi-surface area. We are interested in certain values of $F(n)$—those that are greater than or equal to all previous $F(n)$—so we will redefine the set $\mathcal{A}$ as

$$\mathcal{A} = \{n \in \mathbb{N} : F(k) \leq F(n) \quad \text{for all} \quad k \leq n\}.$$

The set $\mathcal{A}$ lists those volumes that, when factored properly to minimize $s(n)$, have a volume-to-surface-area ratio greater than or equal to that of any smaller volume. By using brute force, involving all possible factorizations for numbers up to 400, we can find and list the first 49 elements of $\mathcal{A}$:

$$\mathcal{A} = \{1, 2, 3, 4, 6, 8, 12, 16, 18, 24, 27, 32, 36, 45, 48, 54, 60, 64, 72, 75, 80, 90, 96, 100, 112, 120, 125, 140, 144, 150, 168, 175, 180, 200, 210, 216, 240, 245, 252, 280, 288, 294, 320, 324, 336, 343, 378, 384, 392, \ldots\}.$$

A longer list of members of $\mathcal{A}$ can also be found in the *On-Line Encyclopedia of Integer Sequences* **[4]**.

We introduce terminology for the optimal side lengths that produce the minimum value for $s(n)$. Define the *best-factored form* of n to be the factorization $x \times y \times z$ where $n = xyz$ and the minimum of $xy + xz + yz$ is achieved.

One point of interest is that finding the best-factored form in three dimensions is not nearly as easy as in the two-dimensional case. In two dimensions, the smaller side is always the greatest factor of n that is less than $\sqrt{n}$. In three dimensions, the natural extension would be to take the greatest factor less than $\sqrt[3]{n}$ as one side, but this does not always work. Easy counterexamples arise from numbers that have a large prime factor, such as 536 $(= 2^3 \times 67)$; the best-factored form for this number is $2 \times 4 \times 67$, even though 8 is the largest factor less than $\sqrt[3]{536}$. However, counterexamples without large prime factors also exist, such as 108 $(= 2^2 \times 3^3)$. The best-factored form for 108 is $3 \times 6 \times 6$, which does not include $4 = \lfloor \sqrt[3]{108} \rfloor$. While $\lfloor \sqrt[3]{n} \rfloor$ seems to be a factor in the best-factored form for every element of $\mathcal{A}$, this remains to be proven, and is left as an open problem for the reader. Fortunately, our analysis will not require a method for finding the best-factored form of any integer.

By brute force, we can rewrite the elements of $\mathcal{A}$ in their best-factored form:

$$\begin{aligned}\mathcal{A} = \{&1 \times 1 \times 1, 1 \times 1 \times 2, 1 \times 1 \times 3, 1 \times 2 \times 2, 1 \times 2 \times 3, 2 \times 2 \times 2, 2 \times 2 \times 3,\\ &2 \times 2 \times 4, 2 \times 3 \times 3, 2 \times 3 \times 4, 3 \times 3 \times 3, 2 \times 4 \times 4, 3 \times 3 \times 4, 3 \times 3 \times 5,\\ &3 \times 4 \times 4, 3 \times 3 \times 6, 3 \times 4 \times 5, 4 \times 4 \times 4, 3 \times 4 \times 6, 3 \times 5 \times 5, 4 \times 4 \times 5,\\ &3 \times 5 \times 6, 4 \times 4 \times 6, 4 \times 5 \times 5, 4 \times 4 \times 7, 4 \times 5 \times 6, 5 \times 5 \times 5, 4 \times 5 \times 7,\\ &4 \times 6 \times 6, 5 \times 5 \times 6, 4 \times 6 \times 7, 5 \times 5 \times 7, 5 \times 6 \times 6, 5 \times 5 \times 8, 5 \times 6 \times 7,\\ &6 \times 6 \times 6, 5 \times 6 \times 8, 5 \times 7 \times 7, 6 \times 6 \times 7, 5 \times 7 \times 8, 6 \times 6 \times 8, 6 \times 7 \times 7,\\ &5 \times 8 \times 8, 6 \times 6 \times 9, 6 \times 7 \times 8, 7 \times 7 \times 7, 6 \times 7 \times 9, 6 \times 8 \times 8, 7 \times 7 \times 8,\\ &\ldots\}.\end{aligned}$$

One pattern we notice, as with almost-squares, is that the three side lengths are all almost (or exactly) equal. For this reason, we will call the elements of $\mathcal{A}$ *almost-cubes*.

A quick glance at the list of almost-cubes in best-factored form shows that taking any two sides of an almost-cube, one seems to have the dimensions of an almost-square. But will this hold as the numbers continue to get larger? This next theorem confirms it. For the proof, it will help to notice that the volume to semi-surface area ratio of any rectangular box of dimensions $n = xyz$ is

$$\frac{xyz}{xy + xz + yz}, \quad \text{which simplifies to} \quad \frac{xy}{xy/z + x + y}.$$

THEOREM 2. *If $n = xyz$ is an almost-cube in best-factored form, then xy, xz, and yz are almost-squares in best-factored form.*

Proof. By symmetry, it is enough to show that xy is an almost-square. Let $n = xyz$ be an almost-cube, and let $k = xy$. Suppose that k is not an almost-square or that k is not in best-factored form. Then there exist $\alpha, \beta \in \mathbb{N}$ so that $\mu = \alpha\beta \leq k$ and

$$\frac{k}{x + k/x} < \frac{\mu}{\alpha + \mu/\alpha}, \quad \text{which easily gives} \quad k\alpha + \frac{k\mu}{\alpha} < \mu x + \frac{k\mu}{x}.$$

However, by the definition of an almost-cube, since $\mu z \leq kz$,

$$\frac{k}{(k/z) + x + (k/x)} \geq \frac{\mu}{(\mu/z) + \alpha + (\mu/\alpha)}.$$

This simplifies to the opposite inequality from the one we derived above, so $k = xy$ is an almost-square in best-factored form. ■

Unfortunately, being the product of numbers where each pair forms an almost-square is not a sufficient condition for being an almost-cube. Rectangular boxes such as $14 \times 19 \times 19$, $18 \times 22 \times 24$, and $19 \times 23 \times 25$ all contain three pairs of almost-squares, but none of them are almost-cubes.

Theorem 2 does imply that there is a limit to how much the largest side of an almost-cube can vary from the smallest side. As with Martin [**2**], triangular numbers come into play. Recall that $T(x)$ represents the number of triangular numbers not exceeding x.

An immediate appeal to Corollary 1 gives us a way to write almost-cubes:

COROLLARY 2. *Almost-cubes can be written in the form* $k(k+h)(k+j)$, *for some* $k, h, j \in \mathbb{N}$ *with* $k \geq 1$ *and* $0 \leq h \leq j \leq T(k)$.

These upper bounds for h and j can be improved. Observation seems to show that $0 \leq h \leq T(k+1) - 1$, but even this tighter upper bound is not tight enough. The upper bound for j can also be improved. Since merely relating almost-cubes to almost-squares on two of their sides will not characterize almost-squares, we now attempt a characterization similar to Martin's. We begin by looking at some special members of the set of almost-cubes.

Punctuation markers

As the reader may have noticed, all of the numbers of the form $m \times m \times m$, $(m-1) \times m \times m$, and $(m-1) \times (m-1) \times m$ seem to be almost-cubes (as intuition suggests). Of course, there are others, but these three seem to be markers—a sort of punctuation of $\mathcal{A}$. We will therefore call numbers of these three forms *punctuation markers.* This leads us to define a *flock* similar to Martin's flocks of almost-squares. A flock is the set of almost-cubes between $(m-1)^3 + 1$ and $m(m-1)^2$, between $m(m-1)^2 + 1$ and $(m-1)m^2$, or between $(m-1)m^2 + 1$ and m^3. We will refer to these as the first, second, and third flocks, respectively. If we wish to discuss *all* numbers k such that $(m-1)^3 < k \leq m(m-1)^2$, without regard to whether they are almost-cubes or not, we will say k is an element of the *range* of the first flock (and similarly for the other two flocks). We can group $\mathcal{A}$ into these flocks and signify the end of a flock with a semicolon to help delineate them:

$$\begin{aligned}\mathcal{A} = \{&1\times1\times1; 1\times1\times2; 1\times1\times3, 1\times2\times2; 1\times2\times3, 2\times2\times2; 2\times2\times3;\\ &2\times2\times4, 2\times3\times3; 2\times3\times4, 3\times3\times3; 2\times4\times4, 3\times3\times4; 3\times3\times5,\\ &3\times4\times4; 3\times3\times6, 3\times4\times5, 4\times4\times4; 3\times4\times6, 3\times5\times5, 4\times4\times5;\\ &3\times5\times6, 4\times4\times6, 4\times5\times5; 4\times4\times7, 4\times5\times6, 5\times5\times5; 4\times5\times7,\\ &4\times6\times6, 5\times5\times6; 4\times6\times7, 5\times5\times7, 5\times6\times6; 5\times5\times8, 5\times6\times7,\\ &6\times6\times6; 5\times6\times8, 5\times7\times7, 6\times6\times7; 5\times7\times8, 6\times6\times8, 6\times7\times7;\\ &5\times8\times8, 6\times6\times9, 6\times7\times8, 7\times7\times7; 6\times7\times9, 6\times8\times8, 7\times7\times8;\\ &\ldots\}.\end{aligned}$$

We show that each punctuation marker is an almost-cube. To do so we must begin with a few quick observations. First,

$$s(n) \geq 3\sqrt[3]{n^2}. \tag{1}$$

This follows immediately from the arithmetic-geometric mean inequality or from basic calculus. Inserting this inequality into the equation for $F(n)$ gives us a second important inquality:

$$F(n) \leq \frac{\sqrt[3]{n}}{3}. \tag{2}$$

Armed with this knowledge, we can now prove that the punctuation markers are almost-cubes. Proving that m^3 is an almost-cube is the easiest: To show that $F(k) \leq F(m^3)$ for all $k \leq m^3$, we simply apply equation (2). This tells us that $F(k) \leq \sqrt[3]{k}/3 \leq m/3 = F(m^3)$, which confirms our first lemma:

LEMMA 1. *Every positive integer of the form m^3 is an almost-cube.*

Martin used a similar process to prove that m^2, $m(m-1)$, and m^2-1 are almost-squares [**2**]. Unfortunately, we cannot continue in the same manner. The upper bound for $F(k)$ given by (2) is actually larger, for some $k < m^2(m-1)$, than $F(m^2(m-1))$. A similar situation arises for $m(m-1)^2$.

To tighten the upper bound for $F(k)$, we increase the lower bound for $s(k)$ given by (1). Let $x \in \mathbb{N}$ be a divisor of k. A simple application of Lagrange multipliers shows that the expression $xy + xz + yz$, subject to the constraint $k = xyz$ with $y, z \in \mathbb{R}^+$, is minimized when $y = z = \sqrt{k/x}$. This gives us $xy + xz + yz \geq k/x + 2\sqrt{kx}$.

If we compute the derivative of the single-variable function $f(x) = k/x + 2\sqrt{kx}$, then we see that it is a decreasing function of x on $0 < x < \sqrt[3]{k}$.

Let d be the largest divisor of k that is less than or equal to $\sqrt[3]{k}$. Also, let $k = abc$ be the best-factored form of k, where $a \leq \sqrt[3]{k}$. Since $a \leq d \leq \sqrt[3]{k}$, we have $s(k) \geq f(a) \geq f(d) = k/d + 2\sqrt{kd}$. This is a tighter lower bound for $s(k)$ than (1), which in turn gives us a tighter upper bound for $F(k)$ than that given by(2), namely

$$F(k) \leq \frac{k}{k/d + 2\sqrt{kd}}. \tag{3}$$

This is the key to the following lemma.

LEMMA 2. *Each positive integer of the form m^3, $m^2(m-1)$, and $m(m-1)^2$ is an almost-cube.*

Proof. We will prove this by induction on m. Note that the first positive numbers of the form $(m-1)^3$, $m(m-1)^2$, and $m^2(m-1)$, namely 1, 2, and 4, are almost-cubes. Also, note that $F(m^3) > F(m^2(m-1)) > F(m(m-1)^2) > F((m-1)^3)$ for every $m \geq 2$. To complete our induction, we need to show that

$$F\big(m(m-1)^2\big) > F(k) \quad \text{whenever} \quad (m-1)^3 < k < m(m-1)^2,$$

$$F\big(m^2(m-1)\big) > F(k) \quad \text{whenever} \quad m(m-1)^2 < k < m^2(m-1),$$

and

$$F(m^3) > F(k) \quad \text{whenever} \quad m^2(m-1) < k < m^3.$$

The most difficult case is the first one, when $(m-1)^3 < k < m(m-1)^2$. In this case, let $a = m(m-1)^2 - k$, so that $1 \leq a < (m-1)^2$. The largest possible factor of k

that is less than or equal to $\sqrt[3]{k}$ is $m-1$. Unfortunately, the simplest idea—taking the other two sides to be $\sqrt{k/(m-1)}$—would create a box with volume-to-surface-area ratio greater than $F(m(m-1)^2)$ if a is small. Thus we need to carefully examine the possible integer divisors of k.

Now, $m-1$ will only divide k if it divides a. If $m-1$ does not divide a, then $m-2$ is the largest possible divisor less than or equal to $\sqrt[3]{k}$, so we can proceed using the bounds from (3). In this subcase,

$$F(k) \leq \frac{m^3-2m^2+m-a}{\frac{m^3-2m^2+m-a}{m-2} + 2(m-2)\sqrt{\frac{m^3-2m^2+m-a}{m-2}}}.$$

We must compare this to $F(m(m-1)^2) = (m^2-m)/(3m-1)$. Letting

$$x = \sqrt{\frac{m^3-2m^2+m-a}{m-2}},$$

we would like to establish the inequality

$$\frac{x}{2+\frac{x}{m-2}} \leq \frac{m^2-m}{3m-1}.$$

Solving for x gives us an equivalent inequality: $x \leq m(1+1/(m^2-3m+1))$. However, replacing a by 1 in the definition of x shows that $x \leq \sqrt{m^2+(m-1)/(m-2)}$. Showing that $\sqrt{m^2+(m-1)/(m-2)} \leq m(1+1/(m^2-3m+1))$ is routine, so this subcase is proved.

If $m-1$ does divide a, then more work is involved. Now k has the form $m^3 - 2m^2+m-b(m-1)$, where $1 \leq b < m-1$. Dividing by $m-1$, we are left with the expression m^2-m-b, which is the product of the remaining divisors. The largest integer value less than $\sqrt{m^2-m-b}$ is $m-2$, and this is the best possible choice for one of the remaining two factors. With these two factors determined, a little algebra shows that

$$F(k) \leq \frac{(m^3-2m^2+m-b(m-1))(m-2)}{3m^3-10m^2+(11-2b)m+3b-4}.$$

We must compare this to $F(m(m-1)^2) = (m^2-m)/(3m-1)$ as above. Substituting 1 for b, since that will maximize $F(k)$, and cross-multiplying, produces the cubic inequality $0 \leq 3m^3-9m^2+8m-2$, which is true for all $m \geq 2$, and the second subcase is proved.

When $m(m-1)^2 < k < m^2(m-1)$, then let $c = m^3-m^2-k$, so that $1 \leq c < m^2-m$. The largest possible factor less than or equal to $\sqrt[3]{k}$ is $m-1$. As before, we compare

$$F(k) \leq \frac{m^3-m^2-c}{\frac{m^3-m^2-c}{m-1} + 2(m-1)\sqrt{\frac{m^3-m^2-c}{m-1}}}$$

to $F(m^2(m-1)) = (m^2-m)/(3m-2)$. Letting

$$y = \sqrt{\frac{m^3-m^2-c}{m-1}},$$

we get the inequality

$$\frac{y}{2+\frac{y}{m-1}} \le \frac{m^2-m}{3m-2},$$

which simplifies to $y \le m$. But this is always true by the definition of y, which proves the second case.

The third case, when $m^2(m-1) < k < m^3$, can be done in a similar fashion, or the result from Lemma 1 can be used. This completes the induction. Therefore, every positive integer of the form m^3, $m^2(m-1)$, and $m(m-1)^2$ is an almost-cube. ■

The characterization begins

Now that we have established the end point of each flock, we would like to take a closer look at the flocks themselves. The first observation we make is that the sum of the three factors is constant within a given flock. Define $p(n) = x + y + z$ where $n = xyz$ is in best-factored form. As with Martin [**2**], we want to determine which boxes of the "correct" $p(n)$ are almost-cubes.

First we make an easy observation. Simple calculus or the arithmetic-geometric mean inequality tells us that $p(n) \ge 3\sqrt[3]{n}$.

Now we determine the largest possible n for a given value of $p(n)$. For instance, if $p(n) = p(m(m-1)^2) = 3m-2$, we know that $n = xy[(3m-2) - x - y]$. We maximize this function in steps, first assuming that x is fixed; taking the derivative with respect to y, we find that n is maximized when $y = ((3m-2) - x)/2$, which gives $n = x((3m-2) - x)^2/2$. We now take the derivative with respect to x and find that n is maximized when $x = m - 2/3$, but this is not an integer. Since we need all three factors to be integers, we look for the values of x nearest to $m - 2/3$ on either side that yield integer factors. If $x = m$, then the other two factors are both $m-1$. If $x = m-1$, then $y = m - 1/2$ is not an integer. If $x = m-2$, then the other two factors are both m. Thus, to find the largest possible n with $p(n) = 3m-2$, we need only compare $m(m-1)^2 = m^3 - 2m^2 + m$ with $m^2(m-2) = m^3 - 2m^2$. Thus, $m(m-1)^2$ is the maximum volume for a box with integer side lengths and $p(n) = 3m-2$.

Similar work shows that the maximum volume obtainable with integer side lengths when $p(n) = 3m-1$ is $m^2(m-1)$; and when $p(n) = 3m$, the maximum is m^3. These will be needed in the following lemma.

LEMMA 3.

- *If n is an almost-cube in the first flock, then* $p(n) = 3m-2$;
- *if n is an almost-cube in the second flock, then* $p(n) = 3m-1$;
- *if n is an almost-cube in the third flock, then* $p(n) = 3m$.

Proof. Suppose that n is an almost-cube in the first flock; then, by definition of an almost-cube, $(m-1)/3 = F[(m-1)^3] \le F(n) = n/s(n) \le (m(m-1)^2)/s(n)$. This means that $s(n) \le 3m^2 - 3m$. Now, if $x+y+z$ is as large as $3m-1$, then using calculus or our intuition we see that $xy + xz + yz \ge 3((3m-1)/3)^2$. So we see that $p(n) = 3m-1$ implies that $s(n) \ge 3m^2 - 2m + 1/3$, which is larger than our upper bound for $s(n)$. Therefore, $p(n) < 3m-1$. The work preceeding the lemma shows that $p(n) \le 3m-3$ implies $n \le (m-1)^3$. Thus, $3m-3 < p(n) < 3m-1$, and so $p(n) = 3m-2$.

The proofs for the other two cases use exactly the same process and are omitted here. ■

Unfortunately, we once again have a necessary but not sufficient condition to be an almost-cube. Even if n has the right $p(n)$, n is not always an almost-cube. For example, let $n = 40 = 2 \times 4 \times 5$. Now when $m = 4$, $m(m-1)^2 = 36 < 40 < 48 = m^2(m-1)$. The sum of the factors for $n = 40$ gives $p(40) = 11 = 3m - 1$, which lies within the bounds given in Lemma 3. However, $n = 40$ is not an almost-cube, as $F(40) = 20/19 < 12/11 = F(36)$.

Next we need to show that given a value for $p(n)$, we can factor n in a useful way. Conversely, we will also show that if we can factor n in this convenient way, then it has a given value for $p(n)$.

LEMMA 4.

- *A positive integer n in the range of the first flock satisfies $p(n) = 3m - 2$ if and only if $n = (m-a-1)(m-b-1)(m+a+b)$ for some integers a and b.*
- *Similarly, a positive integer n in the range of the second flock satisfies $p(n) = 3m - 1$ if and only if $n = (m-c-1)(m-d)(m+c+d)$ for some integers c and d.*
- *Finally, a positive integer n in the range of the third flock satisfies $p(n) = 3m$ if and only if $n = (m-e)(m-f)(m+e+f)$ for some integers e and f.*

Proof. Assume n lies in the range of the first flock and $p(n) = 3m - 2$. Since $p(n) = 3m - 2$ is the sum of factors in the best factorization of n, the factors must clearly have the form $m-a-1$, $m-b-1$, and $m+a+b$ for some integers a and b. This proves one half of the first biconditional statement.

Conversely, assume that $n = (m-a-1)(m-b-1)(m+a+b)$ and in the range of the first flock. Now $n > (m-1)^3$ implies $p(n) > 3m - 3$. The semi-surface area for n is $S = 3m^2 - 4m - a^2 - b^2 - ab - a - b + 1$. Assume $p(n) = 3m - 1$. By the previous lemma, we know $s(n) \geq 3m^2 - 2m + 1/3$, so $s(n) - S \geq 2m + a^2 + b^2 + ab + a + b - 2/3$. Because of ordering, $a \geq 0$. This comes from arbitrarily assigning the first term $(m-a-1)$ to be the smallest. The largest this term can be is $m - 0 - 1 = m - 1$ because making this term any larger will either require $m-b-1$ or $m+a+b$ to be smaller than $m-a-1$, or for the volume to be larger than $m(m-1)^2$.

Case (i) If $b \geq 0$, then $s(n) - S > 0$. This is a contradiction, because $s(n)$ is a lower bound for the semi-surface area. Therefore, $p(n) < 3m - 1$.

Case (ii) If $b < 0$, then $b \geq -a/2$ because of ordering. This comes from assigning the second term $(m-b-1)$ to be the middle of the three sides (not larger than $(m+a+b)$ and not smaller than $(m-a-1)$). Now $b^2 + b \geq 0$ since b is an integer.

Also $a^2 + ab \geq 0$ because $|a| \geq |b|$. Since $2m - 2/3 > 0$ for every m, $s(n) - S > 0$. This is a contradiction as before. Therefore, $p(n) < 3m - 1$.

Since $3m - 3 < p(n) < 3m - 1$, $p(n) = 3m - 2$. This proves the first statement of the theorem. The latter two statements can be proven in exactly the same fashion and are omitted here. ■

Combining Lemmas 3 and 4, we know that an almost-cube n in the first flock has the form $n = (m-a-1)(m-b-1)(m+a+b)$. Thus, we need to set bounds on what a and b can be (similarly for c and d in the second flock and e and f in the third flock). As before, this will involve a little calculus and a lot of algebra. As a reminder, we order the three factors so that $m-a-1 \leq m-b-1 \leq m+a+b$, and similarly for the other two flocks. This implies (among other things) that $a \geq 0$.

We plan to determine how large a can be, as follows: First we determine the b value that, for a given a, yields the largest value for $F(n)$. This will be when b is as negative as possible, which is bounded since we ordered the three sides. This will make the two larger sides as close as possible. We then substitute the value for b into $F(n) \geq F[(m-1)^3]$ and solve for a, where $n = (m-a-1)(m-b-1)(m+a+b)$.

Let

$$\begin{aligned}
p_{1,e} &= 3a^3 + (6m)a^2 + 4(m-1)a - 4(m-1)^2,\\
p_{1,o} &= 3a^3 + (6m)a^2 + (4m-1)a - 2(2m^2 - 3m - 1),\\
p_{2,e} &= (3m-1)c^3 + (6m^2 + 3m - 1)c^2 + (4m^2)c - 4(m^3 - m^2),\\
p_{2,o} &= (3m-1)c^3 + (6m^2 + 3m - 1)c^2 + (8m^2 - 3m + 1)c\\
&\quad - (4m^3 - 6m^2 + 3m - 1),\\
p_{3,e} &= (3m-2)e^3 + (6m^2 - 3m)e^2 - 4m^3,\\
p_{3,o} &= (3m-2)e^3 + (6m^2 - 3m)e^2 + (2-3m)e - (4m^3 - 2m^2 + m),
\end{aligned}$$

where in each label $p_{i,j}$, i represents the appropriate flock and j signifies whether a, c, or e is even or odd. These polynomials will arise from our analysis of the various cases signified by i and j. Let $\alpha_{i,j}$ represent the greatest root of $p_{i,j}$. This root will give us our bounds for a, c, and e.

LEMMA 5.

- *Suppose n is in the first flock. If a is even, the upper bound for a is $\lfloor \alpha_{1,e} \rfloor$. If a is odd, the upper bound for a is $\lfloor \alpha_{1,o} \rfloor$.*
- *Suppose n is in the second flock. If c is even, the upper bound for c is $\lfloor \alpha_{2,e} \rfloor$. If c is odd, the upper bound for c is $\lfloor \alpha_{2,o} \rfloor$.*
- *Suppose n is in the third flock. If e is even, the upper bound for e is $\lfloor \alpha_{3,e} \rfloor$. If e is odd, the upper bound for e is $\lfloor \alpha_{3,o} \rfloor$.*

Proof. Suppose that $n = (m-a-1)(m-b-1)(m+a+b)$ is an almost-cube in the first flock. Our minimum for b occurs when $b = \lfloor -a/2 \rfloor$ (it will be $d = \lfloor (1-c)/2 \rfloor$ and $f = \lfloor (1-e)/2 \rfloor$ for the other two cases). We substitute $b = -a/2$ or $b = -(a+1)/2$ according as a is even or odd. When a is even, the inequality $F(n) \geq F[(m-1)^3]$ is

$$\frac{(m-a-1)\big(m-(-\frac{a}{2})-1\big)\big(m+a+(-\frac{a}{2})\big)}{(m-a-1)\big(m-(-\frac{a}{2})-1\big) + (m-a-1)\big(m+a+(-\frac{a}{2})\big) + \big(m-(-\frac{a}{2})-1\big)\big(m+a+(-\frac{a}{2})\big)} \geq \frac{m-1}{3}$$

and it can be simplified so that

$$\left(\frac{-3}{4}\right)a^3 + \left(\frac{3-9m}{4}\right)a^2 + \left(\frac{3-3m}{2}\right)a + \big(3m^3 - 6m^2 + 3m\big)$$

is greater than or equal to

$$\left(\frac{3-3m}{4}\right)a^2 + \left(\frac{1-m}{2}\right)a + (3m^3 - 7m^2 + 5m - 1).$$

Subtracting to one side, we get the inequality $p_{1,e} \leq 0$. This is true precisely when $a \leq \alpha_{1,e}$. Since a is an integer, we take the greatest integer less than this root. When a is odd, we can solve the same inequality with $b = -(a+1)/2$ instead of $b = -a/2$, giving

$$\frac{(m-a-1)\left(m-\frac{-a-1}{2}-1\right)\left(m+a+\frac{-a-1}{2}\right)}{(m-a-1)\left(m-\frac{-a-1}{2}-1\right)+(m-a-1)\left(m+a+\frac{-a-1}{2}\right)+\left(m-\frac{-a-1}{2}-1\right)\left(m+a+\frac{-a-1}{2}\right)}$$
$$\geq \frac{m-1}{3}.$$

This is true precisely when a is less than the largest root of the cubic $p_{1,o}$, which is $\alpha_{1,o}$. The identical process may be applied to every other case mentioned in the statement of the lemma. The algebra is very straightforward, so we omit it. ∎

Now that we have established bounds for a, c, and e, we now seek to find bounds for b, d, and f. To do so, we will solve the appropriate inequalities for the variables b, d, and f. For example, for the first flock, we solve the inequality $F(n) \geq F[(m-1)^3]$ for b, where $n = (m-a-1)(m-b-1)(m+a+b)$. The other flocks may be completed similarly.

Let

$$\begin{aligned} q_1(a, m) &= (2m + 3a - 2)b^2 + (2am + 2m - 3a^2 - 5a - 2)b \\ &\quad - (m^2 - 2a^2m - 2am - 2m + 2a^2 + 2a + 1), \\ q_2(c, m) &= (2m^2 - 3cm - 3m + c + 1)d^2 + (2cm^2 - 3c^2m - 3cm + c^2 + c)d \\ &\quad - (m^3 - 2c^2m^2 - 2cm^2 - m^2, \end{aligned}$$

and

$$\begin{aligned} q_3(e, m) &= (2m^2 - 3em - m + 2e)f^2 + (2em^2 - 3e^2m - em + 2e^2)f \\ &\quad - (m^2 - 2e^2m^2 + e^2m). \end{aligned}$$

These polynomials come up in our analysis of the first, second, and third flocks, respectively. Let $g_i(x, m)$ be the smaller root of $q_i(x, m)$ and let $h_i(x, m)$ be the larger root of $q_i(x, m)$.

LEMMA 6.

- *For the first flock,*

$$\max\left\{\lfloor -a/2 \rfloor, \lceil g_1(a, m) \rceil\right\} \leq b \leq \min\left\{a, \lfloor h_1(a, m) \rfloor\right\}.$$

- *For the second flock,*

$$\max\left\{\lfloor (1-c)/2 \rfloor, \lceil g_2(c, m) \rceil\right\} \leq d \leq \min\left\{c+1, \lfloor h_2(c, m) \rfloor\right\}.$$

- *For the third flock,*

$$\max\left\{\lfloor (1-e)/2 \rfloor, \lceil g_3(e, m) \rceil\right\} \leq f \leq \min\left\{e, \lfloor h_3(e, m) \rfloor\right\}.$$

Proof. First, we need to remember that because of ordering, $\lfloor -a/2 \rfloor \leq b \leq a$, $\lfloor (1-c)/2 \rfloor \leq d \leq c+1$, and $\lfloor (1-e)/2 \rfloor \leq f \leq e$. By assigning the sides $(m-b-1)$, $(m-d)$, and $(m-f)$ to be the middle of the three side lengths of a rectangular box written in the form given in Lemma 4, these limits prevent this middle term from becoming larger than the last side or smaller than the first side. To complete the proof, simply solve the inequality

$$\frac{(m-a-1)(m-b-1)(m+a+b)}{(m-a-1)(m-b-1)+(m-a-1)(m+a+b)+(m-b-1)(m+a+b)}$$
$$\geq \frac{m-1}{3} = F\left[(m-1)^3\right]$$

for b in terms of a and m. Simplifying, we find that the quantity

$$3(-m+a+1)b^2 + 3(-m(a+1)+a(a+2)+1)b + 3(m^2(m-2)-(a^2-a-1)m+a^2+a)$$

is greater than or equal to

$$(1-m)b^2 + (-am-m+a+1)b + (3m^3-7m^2-a^2m-am+5m+a^2+a-1).$$

This further simplifies to $q_1(a,m) \leq 0$. This will be true when b is between the roots $g_1(a,m)$ and $h_1(a,m)$, which come from subtracting and adding the square root of the discriminant. This process may be repeated for the other two cases in exactly the same way to determine the values for $g_2(c,m)$, $h_2(c,m)$, $g_3(e,m)$, and $h_3(e,m)$. ∎

The final step

It may seem that we have established necessary and sufficient conditions for n to be an almost-cube. Unfortunately, this is not the case. When determining bounds for $\{a, b, c, d, e, f\}$, we always compared the value of $F(n)$ with that of the previous flock leader ($(m-1)^3$, $m(m-1)^2$, or $m^2(m-1)$). However, there still remains the possibility of cancellation *within* the flock. Stated another way, given two potential almost-cubes in the same flock (meeting all the aforementioned conditions of an almost-cube), it may still be possible for $F(n_1) < F(n_2)$ even if $n_2 < n_1$.

One way to alleviate this problem would be to prove the following conjecture:

For all $a, b, c, x, y, z \in \mathbb{N}$, if $a+b+c = x+y+z$ and $abc < xyz$, then

$$\frac{abc}{ab+ac+bc} = \frac{1}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}} < \frac{1}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}} = \frac{xyz}{xy+xz+yz}.$$

Stated another way, given two pairs of three numbers, if their arithmetic means are equal and their geometric means satisfy an inequality, do their harmonic means satisfy a similar inequality? Not surprisingly, this is false. The first counterexample, generated by Martin [**3**], was

$$a = 24, \quad b = 392, \quad c = 9584,$$

and

$$x = 21, \quad y = 506, \quad \text{and} \quad z = 9473.$$

This shows the general statement is false, but the counterexample is quite obviously *not* an almost-cube. This begs the question: if the choices for a, b, c, x, y, and z are sufficiently close to each other as to generate a potential almost-cube, does the conjecture then hold?

Unfortunately, once again the answer is no. Many more counterexamples were recently discovered by Matt DeLong [**1**] and these meet all the previous requirements for an almost-cube. For example, if

$$a = 3307, \quad b = 3323, \quad c = 3370, \quad x = 3303, \quad y = 3329, \quad \text{and} \quad z = 3368,$$

then

$$a + b + c = x + y + z = 10000,$$
$$abc = 37033472570 < 37033473816 = xyz, \quad \text{and}$$
$$F(abc) = 1111.039919\ldots > 1111.03989\ldots = F(xyz).$$

Also, if

$$a = 3309, \quad b = 3320, \quad c = 3371, \quad x = 3301, \quad y = 3332, \quad \text{and} \quad z = 3367,$$

then

$$a + b + c = x + y + z = 10000,$$
$$abc = 37033401480 < 37033404044 = xyz, \quad \text{and}$$
$$F(abc) = 1111.03852\ldots > 1111.03846\ldots = F(xyz).$$

These counterexamples lead us to our final condition, giving us our final set of necessary and sufficient criteria to determine whether a number n is an almost-cube. For computational reasons, we had hoped to find a characterization that would not require comparing any previous integers, but we are unable to accomplish this goal completely. Although we do not need to compare to *all* previous integers, we do need to compare to previous integers *within the range of the same flock.*

THEOREM 3. *Let $n = xyz$ have one of the forms given by Lemma 4 where the appropriate variables a through f satisfy the constraints given in Lemmas 5 and 6. If $F(n) \geq F(k)$ for all $k = rst < n$ where $r + s + t = x + y + z$ and $r, s, t \in \mathbb{N}$, then n is an almost-cube.*

Proof. An n meeting the requirements of Lemmas 4, 5, and 6 will be eligible to be an almost-cube. If $F(n) \geq F(k)$ for all $k = abc < n$ where $a + b + c = x + y + z$, then no cancellation within n's flock occurs. Therefore, n is an almost-cube. ■

A natural conclusion

We have now given necessary and sufficient conditions for an integer to be an almost-cube. While many of the results are not as elegant or compact as in the two-dimensional case, the topic is still a very interesting one to discuss.

Some open problems remain possible areas of research in the future. Some of these areas relate to results that Martin was able to prove and can be extended to almost-cubes. Is there a nice way to find the greatest almost-cube not exceeding n? Is there a nice way to order almost-cubes? Is there a nice way to enumerate almost-cubes? The cancellation concerns would make these last two questions difficult to answer. If we could derive a function that enumerates almost-cubes, we could use it to address the density of almost-cubes.

A somewhat more important problem deals with the bounds for a–f. The roots of the polynomials in Lemmas 5 and 6 are very cumbersome, and so they are not illuminating or easy to work with. Is there a nicer way to represent these values? Also, is it possible not to split apart the two cases for a, c, and e?

We previously mentioned the difficulties of finding the best-factored form of a number n. Is it true of every almost-cube, as it is not for general n, that the greatest factor less than $\sqrt[3]{n}$ is a factor in the best-factored form of n?

A final question depends on the very definition of how we constructed our almost-cubes. The more natural ratio to consider appeared to us to be volume to surface area, but it turned out our flocks were held together by the sum of the side lengths. If we had taken our original ratio to be $F(n) = n/p(n)$, the cancellation concerns within a flock would not have been an issue. Is there a more elegant way to describe these wire frames than some of the expressions found in the description of almost-cubes?

To finish our story from the beginning...

Farmer Ted began his meanderings into the three-dimensional realm of almost-cubes. He soon became fascinated by all the new discoveries he was making. He was able to tell his neighbor that the most efficient way to build his animal cage was to build a 48 ft.^3 cage with side lengths of 3 ft., 4 ft., and 4 ft. His neighbor was so thrilled at the advice Farmer Ted was able to give him, Farmer Ted was made an integral part of the management of the whole farm. Naturally.

Acknowledgment. I would like to thank Matt DeLong for his time, effort, and advice; Greg Martin for his helpfulness and encouragement to tackle this problem; William Ziemer for his help in revising this paper; the two anonymous referees whose suggestions were very beneficial; and the Truth. This research was supported by the Taylor University Science Research Training Program.

REFERENCES

1. Matt DeLong, Three years of trying to prove something false, email to the author, 13 July, 2002.
2. Greg Martin, *Farmer Ted Goes Natural*, this MAGAZINE, **72** (1999), 259–276.
3. ———, Math question, email to the author, 22 July, 1999.
4. N.J.A. Sloane, editor (2004), *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/. ID#=A048874.

Pythagorean Triples and Inner Products

LARRY J. GERSTEIN
University of California
Santa Barbara, CA 93106-3080
gerstein@math.ucsb.edu

Linear algebra over rings—particularly over $\mathbb{Z}$—is a fascinating topic that straddles course boundaries and can help bridge the present unnecessary gap between introductions to algebra and number theory. Moreover, a brief introduction to integral linear algebra can be helpful in further studies. For example, in both coding theory and solid state physics one is led to study *lattices* over the integers—roughly speaking, periodic discrete arrays of points in space (a more precise definition will be given below)—for which the standard linear algebra curriculum, dealing only with *spaces*, is inadequate. We refer the reader to the books by Conway–Sloane **[3]** or Ebeling **[6]** for lattices in coding theory, and Kittel **[7]** or Senechal **[14]** for lattices in solid state physics.

Following the introduction, we review inner product spaces and the representation of inner products by symmetric matrices. The inner products we study will not necessarily be positive definite. (Indeed, our coefficients will not always be real or complex numbers.) In a background section, we introduce unimodular matrices over $\mathbb{Z}$ and then $\mathbb{Z}$-lattices on rational inner product spaces; and then we explore the fundamental role of unimodular matrices in connection with basis changes for lattices.

The following section is the heart of the article. There we give a new perspective on Pythagorean triples through the medium of lattices on inner product spaces, using the machinery of the earlier sections. A *Pythagorean triple* is a triple (a, b, c) of integers such that $a^2 + b^2 = c^2$; and the triple (a, b, c) is *primitive* if $\gcd(a, b, c) = 1$. The construction of primitive Pythagorean triples, and in particular the demonstration that there are infinitely many of them, is a truly ancient subject and a standard topic in elementary number theory courses.

We will give a new proof of a theorem from 1894 by Leonard Eugene Dickson (a theorem that appeared in Volume 1 of the *American Mathematical Monthly* **[4]**) on the representation of primitive Pythagorean triples—a representation that does not seem to be widely known today—and then deduce some consequences. Underlying our proof of Dickson's theorem is the observation that the entries in a primitive Pythagorean triple are the coefficients of certain vectors in an appropriate inner product space with respect to a particular basis; then changing to a more convenient basis instantly yields the description in Dickson's theorem.

In the penultimate section, we will have a brief look at Pythagorean triples over other rings, and we'll conclude with remarks on other approaches to Pythagorean triples.

Background

We will introduce only those properties of lattices that we need. For thorough introductions to lattices on inner product spaces, see the books of Cassels **[2]** and O'Meara **[10]**. Basic notations: $M_n(R)$ denotes the set of all $n \times n$ matrices with entries in whatever domain R is under discussion; and $GL_n(R)$ denotes the group of matrices in $M_n(R)$ that have inverses also in $M_n(R)$. For example,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in GL_n(\mathbb{R}) \quad \text{but} \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \notin GL_n(\mathbb{Z}).$$

The expression $\langle\alpha_1, \ldots, \alpha_n\rangle$ denotes a diagonal matrix with the listed elements as its diagonal. The symbols $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Q}$ respectively denote the integers, the real numbers, and the rational numbers. Finally, if R is a ring then R^* denotes its group of units.

Inner product spaces The dot product on $\mathbb{R}^n$ is an important example of a wider class of useful functions that we will introduce in this section. Let V be an n-dimensional vector space over a field F of characteristic not 2. (The theory when char $F = 2$ is rather different, and we won't need it.) A mapping $B : V \times V \to F$ is a *bilinear form* on V if it is linear in each variable when the other is held fixed. And B is *symmetric* if $B(x, y) = B(y, x)$ for all $x, y \in V$. We will call a symmetric bilinear form an *inner product*, and the related mapping $q : V \to F$ defined by $q(x) = B(x, x)$ is the *quadratic form* associated with B. (Why *quadratic*? Because $q(\alpha x) = \alpha^2 q(x)$ for all $\alpha \in F$.) With this additional structure V is said to be a *quadratic space* over F, a *quadratic F-space*, or an *inner product space* over F.

EXAMPLES.

(i) The term *inner product* is derived from the classical example in which B is the dot product on Euclidean space $\mathbb{R}^n$, though the term is used in dramatically different settings as well. And in this space we have $q(x) = \sum x_i^2$, the *squared length* of $x = (x_1, \ldots, x_n)$.

(ii) On $\mathbb{R}^4$, define $B(x, y) = x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4$. The resulting quadratic $\mathbb{R}$-space is *Minkowski space*, useful in special relativity. Notice that in this space, unlike the preceding example, there are nonzero vectors v—such as $(1, 0, 0, 1)$—with the property that $q(v) = 0$. Vectors with this property in a quadratic space are said to be *isotropic.* (Physicists call the collection of isotropic vectors in Minkowski space the *light cone* of the space.)

Now suppose V is a quadratic F-space with basis $\mathbb{B} = \{v_1, \ldots, v_n\}$, and let B be an inner product on V. The symmetric matrix $A = (a_{ij}) \in M_n(F)$ defined by $a_{ij} = B(v_i, v_j)$ is the *Gram matrix* of V with respect to $\mathbb{B}$; we write $V \sim A$ with respect to $\mathbb{B}$. Conversely, given the vector space V, a basis $\mathbb{B} = \{v_1, \ldots, v_n\}$, and your favorite symmetric matrix $A = (a_{ij}) \in M_n(F)$, we can *define* a bilinear form B on V by setting $B(v_i, v_j) = a_{ij}$ and, more generally, by setting $B(\sum_i \alpha_i v_i, \sum_j \beta_j v_j) = \sum_{i,j} \alpha_i \beta_j a_{ij}$ for all $\alpha_i, \beta_j \in F$. This gives V the structure of a quadratic F-space, and $V \sim A$ with respect to $\mathbb{B}$.

Unimodular matrices Suppose A is an $n \times n$ matrix with integer entries. Under what conditions does A have an inverse whose entries are integers? That is, when is $A \in GL_n(\mathbb{Z})$? Certainly, if $A \in GL_n(\mathbb{Z})$, then the equation $AA^{-1} = I_n$ and the multiplicative property of the determinant forces $\det A$ to be ± 1. Conversely, suppose $\det A = \pm 1$. Recall that the *adjoint* formula for A^{-1} expresses the entries of A^{-1} as certain signed subdeterminants of A divided by $\det A$. From this it follows immediately that $A^{-1} \in M_n(\mathbb{Z})$. Thus $A \in GL_n(\mathbb{Z})$ if and only if $\det A \in \mathbb{Z}^* = \{\pm 1\}$. Elements of $GL_n(\mathbb{Z})$, which stands for the *general linear group* over $\mathbb{Z}$, are called *unimodular* matrices over $\mathbb{Z}$.

Lattices on inner product spaces Assume V is an n-dimensional inner product space over $\mathbb{Q}$, and for some $k \leq n$ let $\mathbb{B} = \{v_1, \ldots, v_k\}$ be a linearly independent subset of V. The set L of linear combinations of these vectors having *integer* coefficients is the *$\mathbb{Z}$-lattice* in V with basis $\mathbb{B}$. In symbols: $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k$. If $k = n$, and hence L spans V, we say L is *on* V. [Note: In solid state physics sometimes the word *basis* is given a different meaning. Namely, given a lattice in $\mathbb{R}^3$, imagine congruent configurations of atoms located at each of the lattice points, producing a space-filling crystal structure. The physicists call one of those configurations the "basis" associated with the crystal.]

If A is the Gram matrix of the inner product with respect to $\mathbb{B}$, we write $L \sim A$ with respect to $\mathbb{B}$.

Now suppose L is a lattice on V, with $\mathbb{B} = \{v_1, \dots, v_n\}$ a basis for L (and hence for V). Suppose $\mathbb{B}' = \{v'_1, \dots, v'_n\}$ is another basis for V, with $T = (t_{ij}) \in GL_n(\mathbb{Q})$ the matrix for the transition $\mathbb{B} \to \mathbb{B}'$; that is, $v'_j = \sum_i t_{ij} v_i$, for $1 \leq j \leq n$. Then we claim that $\mathbb{B}'$ is a basis for L if and only if $T \in GL_n(\mathbb{Z})$. To see this, first suppose $\mathbb{B}'$ is a basis for L. Then $T \in M_n(\mathbb{Z})$ because $\mathbb{B}' \subseteq L$; and since T^{-1} is the matrix for the transition $\mathbb{B}' \to \mathbb{B}$ we also have $T^{-1} \in M_n(\mathbb{Z})$, proving the claim. Conversely, if T is unimodular, then $\mathbb{B}'$ is a basis for V contained in L, so $\mathbb{B}'$ spans a sublattice M of L. But if $T^{-1} = (s_{ij})$ then $v_j = \sum_i s_{ij} v'_i$, hence $\mathbb{B} \subseteq M$, and so $M = L$, and we are done.

It follows from this discussion that if $w \in L$, say $w = \sum_i a_i v_i$, then for w to extend to a basis for L it is necessary that $\gcd(a_1, \dots, a_n) = 1$; this is because the transpose of $(a_1, \dots, a_n)$ would serve as a column vector of some unimodular transition matrix and if there were a common integer divisor in the column, it would also be a divisor of the determinant. In fact this condition is sufficient as well, because every column vector of relatively prime integers can be completed to a unimodular matrix. (See Newman [**9**, pp. 13–14] or Rotman [**13**, pp. 260–261] for a proof.) A vector w with this property is called a *primitive* vector of L.

It follows that if w is a primitive vector of L and $\alpha \in \mathbb{Q}$, then $\alpha w \in L$ if and only if $\alpha \in \mathbb{Z}$. Notice also that every line (that is, 1-dimensional subspace) in V contains a primitive vector of L, and that vector is unique "up to sign," by which we mean, "up to factors in $\mathbb{Z}^* = \{\pm 1\}$." To see this, suppose $0 \neq v = \sum_i \alpha_i v_i \in V$. Multiply v by a common denominator of the α_i to get a vector $\sum_i a_i v_i \in L$, then divide by $\gcd(a_1, \dots, a_n)$ to get a primitive vector w of L in the line $\mathbb{Q}v$; then the only primitive vectors of L in that line are of the form εv with $\varepsilon \in \mathbb{Z}^*$. Incidentally, we have written $\mathbb{Z}^*$ here instead of $\{\pm 1\}$ to facilitate the extension of these results to other rings, a topic we pursue later in this paper.

Lattices and Pythagorean triples

Suppose V is a 3-dimensional quadratic space over $\mathbb{Q}$ with basis $\mathbb{B} = \{v_1, v_2, v_3\}$, and suppose further that $V \sim \langle 1, 1, -1 \rangle$ with respect to $\mathbb{B}$. Let $L = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \mathbb{Z}v_3$, and suppose $v = av_1 + bv_2 + cv_3 \in L$. Then $q(v) = a^2 + b^2 - c^2$. Therefore (a, b, c) is a Pythagorean triple if and only if v is isotropic (that is, $q(v) = 0$); and (a, b, c) is primitive if and only if v is a primitive vector in L. Thus *determining the primitive Pythagorean triples is equivalent to determining the primitive isotropic vectors in L.*

Now define a new basis $\mathbb{B}' = \{w_1, w_2, w_3\}$ for L by

$$w_1 = v_1 + v_3, \quad w_2 = v_2 + v_3, \quad \text{and} \quad w_3 = v_1 + v_2 + v_3.$$

Here w_1 and w_2 are clearly primitive isotropic vectors, so we're on the right track! And the fact that $\mathbb{B}'$ is a basis for L follows from the observation that the transition matrix

$$T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

for the change $\mathbb{B} \to \mathbb{B}'$ is unimodular. If $w = aw_1 + bw_2 + cw_3 = (a+c)v_1 + (b+c)v_2 + (a+b+c)v_3$, then $q(w) = c^2 - 2ab$. Thus, we have

$$L \sim \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{with respect to} \quad \{w_1, w_2, w_3\}.$$

This new description of L will turn out to yield the characterization of primitive Pythagorean triples that we are after, because it will enable us to systematically list primitive isotropic vectors of L and their associated Pythagorean triples. (The list is infinite; we will truncate due to exhaustion, not because we don't know how to extend our list.)

If $v = rw_1 + sw_2 + tw_3$ then $q(v) = -2rs + t^2$, hence

$$v \text{ is isotropic} \iff t^2 = 2rs.$$

It follows that v is *primitive* and isotropic if and only if $t^2 = 2rs$ and $\gcd(r, s) = 1$. Assuming these conditions to hold, then

$$\begin{aligned} v &= rw_1 + sw_2 + tw_3 \\ &= r(v_1 + v_3) + s(v_2 + v_3) + t(v_1 + v_2 + v_3) \\ &= (r+t)v_1 + (s+t)v_2 + (r+s+t)v_3 \end{aligned}$$

and therefore

$$(r+t, \quad s+t, \quad r+s+t)$$

is the associated primitive Pythagorean triple. We have now proved the following result of Dickson [**4**]:

THEOREM. *The triple $(a, b, c) \in \mathbb{Z}^3$ is a primitive Pythagorean triple if and only if*

$$(a, b, c) = (r+t, \quad s+t, \quad r+s+t)$$

for some integers r, s, t satisfying $\gcd(r, s) = 1$ *and* $t^2 = 2rs$. *Moreover, the correspondence $(a, b, c) \longleftrightarrow (r, s, t)$ is a bijection.*

Notice that the primitive isotropic vectors $\pm w_1$ correspond via the theorem to the trivial Pythagorean triples $(\pm 1, 0, \pm 1)$; similarly, the vectors $\pm w_2$ correspond to the triples $(0, \pm 1, \pm 1)$.

In exhibiting primitive Pythagorean triples, as in the accompanying table, one is usually interested only in Pythagorean triples $(a, b, c) = (r+t,\ s+t,\ r+s+t)$ for which a, b, c are all positive. Clearly this is the case if r, s, t are all positive. Conversely, if a, b, c are positive then we claim that r, s, t are positive as well. The inequalities $a < c$ and $b < c$ imply $s > 0$ and $r > 0$, respectively. Suppose $t \leq 0$. Since $r + t = a > 0$, we have $r > -t \geq 0$; similarly, $s > -t$. Hence $rs > t^2$, contradicting the fact that $2rs = t^2$. Thus r, s, and t must all be positive, as claimed.

Also, notice that the conditions $\gcd(r, s) = 1$ and $t^2 = 2rs$ in the theorem force t to be even and one of r, s to be twice a square and the other an odd square. In the table all these conditions are in place, with t growing as we move from top to bottom. Interchanging given values of r and s would just interchange the associated a and b, so we will assume throughout that $r > s$, hence obtaining $a > b$. Except for that, for each value of t all the possibilities for r and s are displayed. If a given t has k distinct prime divisors, then there are 2^k ways to choose positive r and s satisfying the conditions of the theorem, and hence 2^{k-1} lines associated with t in the table.

TABLE 1: Pythagorean triples listed in order of t

t	$t^2/2$	r	s	(a, b, c)
2	2	2	1	(4, 3, 5)
4	8	8	1	(12, 5, 13)
6	18	18	1	(24, 7, 25)
		9	2	(15, 8, 17)
8	32	32	1	(40, 9, 41)
10	50	50	1	(60, 11, 61)
		25	2	(35, 12, 37)
12	72	72	1	(84, 13, 85)
		9	8	(21, 20, 29)
14	98	98	1	(112, 15, 113)
		49	2	(63, 16, 65)
16	128	128	1	(144, 17, 145)
18	162	162	1	(180, 19, 181)
		81	2	(99, 20, 101)
20	200	200	1	(220, 21, 221)
		25	8	(45, 28, 53)
22	242	242	1	(264, 23, 265)
		121	2	(143, 24, 145)
24	288	288	1	(312, 25, 313)
		32	9	(56, 33, 65)
26	338	338	1	(364, 27, 365)
		169	2	(195, 28, 197)
28	392	392	1	(420, 29, 421)
		49	8	(77, 36, 85)
30	450	450	1	(480, 31, 481)
		225	2	(255, 32, 257)
		50	9	(80, 39, 89)
		25	18	(55, 48, 73)
32	512	512	1	(544, 33, 545)

REMARK. If (r, s, t) satisfies the conditions of the theorem (that is, $\gcd(r, s) = 1$ and $t^2 = 2rs$) and λ belongs to the multiplicative monoid

$$\{\lambda \in \mathbb{Z} \mid \gcd(\lambda, t) = 1\}$$

then $(r, \lambda^2 s, \lambda t)$ and $(\lambda^2 r, s, \lambda t)$ also satisfy the theorem conditions and therefore again lead to primitive Pythagorean triples. For example, from $(r, s, t) = (2, 1, 2)$ one gets the Pythagorean triple $(4, 3, 5)$ (the top line inside the table); and then the choice $\lambda = 3$ gives $(r, \lambda^2 s, \lambda t) = (2, 9, 6)$, yielding the Pythagorean triple $(8, 15, 17)$, while $(\lambda^2 r, s, \lambda t) = (18, 1, 6)$ produces $(24, 7, 25)$. Similarly, the choice $\lambda = 5$ leads from the Pythagorean triple $(4, 3, 5)$ to the triples $(12, 35, 7)$ and $(60, 11, 61)$. This suggests some graphical and algebraic structures on the set of primitive Pythagorean triples, topics explored much more fully in the recent paper by McCullough [**8**]. We will refer again to McCullough's work in the final section.

The observation that all the triples we have produced have the form $(a, b, a + s)$ leads to the following corollary.

COROLLARY 1. *Suppose s is a positive integer that is either an odd square or twice a square. Then there are infinitely many primitive Pythagorean triples of the form $(a, b, a + s)$ with $a, b > 0$.*

Proof. Let r be any positive integer relatively prime to s having the property that $2rs$ is a square, and set $t = \sqrt{2rs}$. Then from the theorem it follows that

$$(a, b, c) = (r + t,\ s + t,\ r + t + s)$$

is a primitive Pythagorean triple. Since there are infinitely many possibilities for r, we are done. ■

Given a primitive Pythagorean triple (a, b, c), the associated integers r, s, t are given by

$$t = a + b - c, \qquad r = c - b, \quad \text{and} \quad s = c - a.$$

In Corollary 1 we used conditions on r and s to show existence of certain Pythagorean triples. Now let's move in the opposite direction, starting with known information on Pythagorean triples.

COROLLARY 2. *There are infinitely many pairs of consecutive positive integers such that one is an odd square and the other is twice a square.*

Proof. It was shown by Fermat that there are infinitely many Pythagorean triples (a, b, c) such that $a - b = \pm 1$. (Sierpiński [**15**, Chapter II, §4] gives the proof.) But with the associated r, s as in our theorem we then have $r - s = a - b = \pm 1$, so the pairs $\{r, s\}$ satisfy the conclusion. ■

How can we generate the pairs $\{r, s\}$ whose existence is guaranteed in Corollary 2? Our results give a bijection between these pairs and the Pythagorean triples (a, b, c) of positive integers for which $a - b = \pm 1$. Fermat showed that the full sequence of these Pythagorean triples (except for interchanges of a and b) can be produced as follows. Set $T_1 = (3, 4, 5)$; and having produced $T_n = (a_n, b_n, c_n)$ with $a_n - b_n = \pm 1$, define $T_{n+1} = (a_{n+1}, b_{n+1}, c_{n+1})$ by the equations

$$a_{n+1} = 3a_n + 2c_n + 1, \quad b_{n+1} = a_{n+1} + 1, \quad \text{and} \quad c_{n+1} = 4a_n + 3c_n + 2.$$

With the sequence $\{T_n\}_{n\in\mathbb{N}}$ in hand, we can produce the sequence of pairs $\{r_n, s_n\}_{n\in\mathbb{N}}$ by the formulas $r_n = c_n - b_n$ and $s_n = c_n - a_n$. Here is a table with the first few values.

n	a_n	b_n	c_n	r_n	s_n
1	3	4	5	1	2
2	20	21	29	$8 = 2 \cdot 2^2$	$9 = 3^2$
3	119	120	169	$50 = 2 \cdot 5^2$	$49 = 7^2$
4	696	697	985	$288 = 2 \cdot 12^2$	$289 = 17^2$
5	4059	4060	5741	$1681 = 41^2$	$1682 = 2 \cdot 29^2$
6	23660	23661	33461	$9801 = 99^2$	$9800 = 2 \cdot 70^2$
7	137903	137904	195025	$57121 = 239^2$	$57122 = 2 \cdot 169^2$
8	803760	803761	1136689	$332928 = 2 \cdot 408^2$	$332929 = 577^2$

We note that Corollary 2 is not new. In fact, the Diophantine equations of the form $x^2 - Dy^2 = \pm 1$, with D a nonsquare positive integer, are the *Pell equations*, and their study has a lengthy, rich, and multifaceted history. It is well known that a Pell equation has infinitely many integer solutions (in fact, the solutions to $x^2 - Dy^2 = 1$ form an infinite cyclic group with respect to a suitable multiplication); and when $D = 2$, Corollary 2 is an instance of this theorem. Texts by Sierpiński [**15**, Chapter 2, § 17], Silverman [**16**, Chapters 29–31], and Burton [**1**, Chapter 14] all give the details. As an illustration of the history, we note that line 8 of the preceding table leads to 577/408 as an approximation of $\sqrt{2}$, an estimate known to the Hindu mathematician Baudhâyana around 400 B.C.E. See Dickson's *History of the Theory of Numbers* [5, pp. 341–400], for more of this kind of background. Also see the references in Robson [12].

Other rings

What about Pythagorean triples over other commutative rings? The reader can easily check that if R is any commutative ring, and elements $r, s, t \in R$ satisfy the equation $t^2 = 2rs$ that emerged in the preceding section, then $(a, b, c) = (r + t,\ s + t,\ r + s + t)$ is a Pythagorean triple; that is, $a^2 + b^2 = c^2$. There remains the question of whether these are all the Pythagorean triples over R, and also the issue of primitivity. We will not pursue these matters over arbitrary commutative rings, but here are a few observations.

First note that if $\operatorname{char} R = 2$, then the Pythagorean triples are just the triples $(a, b, a + b) \in R^3$, so the subject is trivial.

Now suppose $\operatorname{char} R \neq 2$, and suppose further that R is a principal ideal domain with quotient field $F \neq R$. Then the material on $\mathbb{Z}$-lattices in the early sections, through the theorem, carries over virtually word for word using R instead of $\mathbb{Z}$ and F instead of $\mathbb{Q}$. Thus we have R-lattices on quadratic F-spaces, unimodular R-matrices, primitive vectors, and so on; and in particular the theorem holds in this wider context. Also note that if (a, b, c) is a primitive Pythagorean triple in R^3, then so are $(\sigma(a), \sigma(b), \sigma(c))$ for every automorphism σ of R and $(\varepsilon a, \varepsilon b, \varepsilon c)$ for all $\varepsilon \in R^*$. And a primitive Pythagorean triple over any principal ideal domain that is a subring of R is a primitive Pythagorean triple over R as well.

EXAMPLE 1. Suppose $R = k[x]$, with k a field of characteristic not 2. We want to choose instances of (r, s, t) satisfying the conditions of our theorem and use these to construct primitive Pythagorean triples over R. Here, since 2 is a unit, the word "even" is redundant. Hence, to construct nontrivial triples we can let t be any nonzero element of $k[x]$.

(i) Suppose $t = 1$. (So without having made any further choices it is already clear that any resulting Pythagorean triple will be in k^3.) Choose $r \in k^* = k - \{0\}$ at random, and put $s = 1/2r$. Then upon writing down $(r + 1, s + 1, r + s + 1)$ and clearing denominators to simplify our expression, we get the associated primitive Pythagorean triple

$$(2r^2 + 2r,\ 2r + 1,\ 2r^2 + 2r + 1)$$

Here "clearing denominators" did not fundamentally change the triple, since it meant multiplying each term of the triple by a common element of $R^* = k^*$. In particular, it preserved the primitivity of the triple.

(ii) Here is a short table in the style of the table of the preceding section with some further examples over $k[x]$. (To conserve space, we omit the column for $t^2/2$.)

t	r	s	(a, b, c)
x	$\frac{x^2}{2}$	1	$(x^2 + 2x,\ 2x + 2,\ x^2 + 2x + 2)$
$x(x+1)$	$\frac{x^2(x+1)^2}{2}$	1	$(x^4 + 2x^3 + 3x^2 + 2x,\ 2x^2 + 2x + 2,\ x^4 + 2x^3 + 3x^2 + 2x + 2)$
	$\frac{x^2}{2}$	$(x+1)^2$	$(3x^2 + 2x,\ 4x^2 + 6x + 2,\ 5x^2 + 6x + 2)$

EXAMPLE 2. $R = \mathbb{Z}[i]$, the ring of Gaussian integers. Here, as over $\mathbb{Z}$, we must have $2 \mid t^2$. This is equivalent to the condition $(1+i) \mid t$, since 2 is an associate of $(1+i)^2$ and $1+i$ is prime. (See Pollard–Diamond [**11**, Chapter 2].) In keeping with the remarks at the start of this section, in the following short table of primitive Pythagorean triples over $\mathbb{Z}[i]$ with $|t|$ small, we will omit triples in $\mathbb{Z}^3$ and conjugates of listed triples. Also, if (a, b, c) has been listed, then (a, ci, bi) and (c, ai, bi) (and other similarly derived triples) are automatically qualified for listing as well, and hence are omitted from the table. Finally, we omit triples in which some entry is 0.

t	$t^2/2$	r	s	(a, b, c)
$1+i$	i	i	1	$(1+2i,\ 2+i,\ 2+2i)$
2	2	$2i$	$-i$	$(2+2i,\ 2-i,\ 2+i)$
$2+2i$	$4i$	$4i$	1	$(2+6i,\ 3+2i,\ 3+6i)$
$3+i$	$4+3i$	$4+3i$	1	$(7+4i,\ 4+i,\ 8+4i)$
$3+9i$	$-36+27i$	$-36+27i$	1	$(-33+36i,\ 4+9i,\ -32+36i)$
		$3+4i$	$9i$	$(6+13i,\ 3+18i,\ 6+22i)$

Other approaches to Pythagorean triples

Let's conclude by briefly reconciling the description of primitive Pythagorean triples over $\mathbb{Z}$ given in this article with other treatments. According to our theorem and the subsequent paragraph, the primitive triples with positive entries have the form $(a, b, c) = (r+t, s+t, r+s+t)$ with $r = 2u^2$ and $s = v^2$ (or vice versa) for some $u, v \in \mathbb{Z}$, with v odd. Moreover $t^2 = 2rs = 4u^2v^2$, and so $t = 2uv$. Now set $m = u + v$ and $n = u$. Then it is easily checked that

$$(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2).$$

This is the usual representation of primitive Pythagorean triples found in the literature. See Burton [**1**], for example.

Quite a different approach to Pythagorean triples can be found in the recent work of McCullough [**8**]. (Also see the references in that paper.) As we have mentioned, from the equation $(a, b, c) = (r+t, s+t, r+s+t)$ in our theorem, we have $t = a + b - c$, $r = c - b$, and $s = c - a$. When $a, b > 0$, the value t is what McCullough calls the *excess* of the triple: the amount by which the sum of the leg lengths of a right triangle exceeds the length of the hypoteneuse; and r is McCullough's *height*. McCullough uses the excess and height to derive a parameterization for triples that ultimately leads to a group structure on the collection of primitive Pythagorean triples.

One can also approach Pythagorean triples through the study of integral points on curves, and the reader can see an introduction to this approach in Silverman [**16**, Chapter 3].

Whether one prefers to produce Pythagorean triples by considering lattices on inner product spaces, as has been our approach, or by some other method, the remarkable diversity of possibilities is certainly a testament to the continuing appeal of the subject.

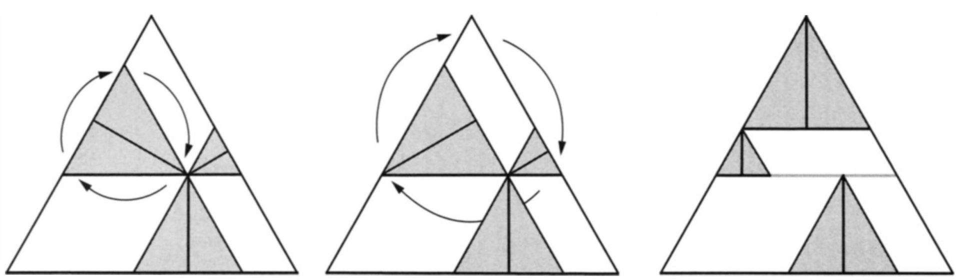
REFERENCES

1. David M. Burton, *Elementary Number Theory*, McGraw-Hill, New York, 2002.
2. J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, New York, 1978.
3. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups* (3rd edition), Springer-Verlag, New York, 1999.

4. L. E. Dickson, Lowest integers representing sides of a right triangle, *Amer. Math. Monthly* **1** (1894), 6–11.
5. ———, *History of the Theory of Numbers*, Vol. 2, Chelsea Pubishing Company, New York, 1971.
6. Wolfgang Ebeling, *Lattices and Codes*, 2nd ed., Friedr. Vieweg & Sohn, Braunschweig/Wiesbaden, 2002.
7. Charles Kittel, *Introduction to Solid State Physics*, 7th ed., John Wiley & Sons, New York, 1996.
8. Darryl McCullough, Height and excess of Pythagorean triples, this MAGAZINE, to appear.
9. Morris Newman, *Integral Matrices*, Academic Press, New York, 1972.
10. O. Timothy O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, New York, 2000.
11. H. Pollard and H. G. Diamond, *The Theory of Algebraic Numbers*, Mathematical Association of America, 1975.
12. E. Robson, Words and pictures: New light on Plimpton 322, *Amer. Math. Monthly* **109** (2002), 105–120.
13. Joseph J. Rotman, *Advanced Modern Algebra*, Prentice-Hall, Upper Saddle River, 2002.
14. Marjorie Senechal, *Quasicrystals and Geometry*, Cambridge University Press, 1995.
15. W. Sierpiński, *Elementary Theory of Numbers*, North-Holland, New York, 1988.
16. J. H. Silverman, *A Friendly Introduction to Number Theory*, 2nd ed., Prentice-Hall, Upper Saddle River, 2001.

Proof Without Words: Viviani's Theorem

In an equilateral triangle, the sum of the distances from any interior point to the three sides is equal to the altitude of the triangle.



——KEN-ICHIROH KAWASAKI
NARA UNIVERSITY OF EDUCATION
TAKABATAKE-CHO, NARA
630–8528, JAPAN

NOTES

Wafer in a Box

RALPH ALEXANDER
JOHN E. WETZEL
University of Illinois at Urbana-Champaign
Urbana, IL 61801-2975
jralex@math.uiuc.edu
j-wetzel@uiuc.edu

We consider the following interesting "fitting" question, asked recently by Jerrard et al. [7]:

Wafer in a box. What is the radius of the largest disk that fits in a given box?

An answer would provide a necessary and sufficient condition on the positive reals a, b, c, and ρ for a disk of radius ρ to fit in an $a \times b \times c$ box, in the spirit of Post's 1993 necessary and sufficient condition on the six sides for one triangle to fit into another [8]. Our argument makes use of the "penny in a corner" problem from the 1948 William Lowell Putnam Mathematical Competition [9], for which we give a simple solution.

Preliminaries It will be convenient to call a closed disk with zero thickness in $\mathbb{R}^3$ a *wafer* and to think of it as a thin tile that one can move physically in space. We say that the wafer ω of radius ρ *fits* in the $a \times b \times c$ box if the box has a subset that is geometrically congruent to ω.

We begin with a useful preliminary observation: If a wafer fits in a box in any way whatsoever, then it also fits in the box with its center at the center of symmetry of the box. Indeed, if a wafer ω lies in the box, then the wafer ω' obtained by reflecting it through the center S of symmetry of the box also lies in the box (FIGURE 1) and (by convexity) so does the *cylinder* having ω and ω' as ends. The midsection of this cylinder (parallel to and midway between the end disks) is a wafer with center at S that is congruent to ω, and it clearly lies in the box.

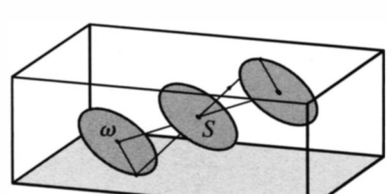


Figure 1 Centering

We say that a wafer ω is *centered* if its center lies at the center S of symmetry of the box. The radius ρ of a centered wafer that fits in an $a \times b \times c$ box clearly cannot exceed the distance from the center S to any edge of the box, and we have the inequality

$$\rho \leq \frac{1}{2} \min \left\{ \sqrt{a^2 + b^2}, \sqrt{b^2 + c^2}, \sqrt{c^2 + a^2} \right\}. \quad (1)$$

(Indeed, the projection of the wafer onto a face of the box is an ellipse—possibly degenerate—whose major axis is equal to the diameter of the wafer.)

Compactness considerations show that there is a largest wafer that fits in the box, and we may suppose that it is centered. A wafer that lies entirely in the interior of the box is obviously not maximal. If a centered wafer touches one face of the box, then it must also touch the face opposite, at the point symmetrically located. No centered wafer that touches just two opposite faces of the box can be maximal, because a small rotation about a suitable axis through S would move it into the interior of the box. Consequently there are just two possibilities for a maximal centered wafer: (1) it touches exactly four faces (two pairs of opposite faces) of the box, or (2) it touches all six faces of the box.

Finally, suppose a centered wafer ω with radius ρ touches both $x \times y$ faces of an $a \times b \times c$ box (where (x, y, z) is a permutation of (a, b, c)). Then ρ must be at least the distance to that face:

$$\rho \geq \frac{1}{2} z. \quad (2)$$

Long boxes At this point it is convenient to separate long boxes from short ones. Suppose the notation is chosen so that c is the longest edge. We call the box *long* if $c > \sqrt{a^2 + b^2}$. For a long box, inequality (1) becomes

$$\rho \leq \frac{1}{2} \sqrt{a^2 + b^2}. \quad (3)$$

If a maximal centered wafer ω of radius ρ touches the two $a \times b$ faces of a long box, then it follows from (2) and (3) that

$$c > \sqrt{a^2 + b^2} \geq 2\rho \geq c,$$

a contradiction. Consequently a maximal centered wafer in a long box touches just the two $a \times c$ faces and the two $b \times c$ faces. A wafer of radius $\frac{1}{2}\sqrt{a^2 + b^2}$ fits diagonally (FIGURE 2), and according to (3) no larger wafer fits. It follows that the largest wafer that fits in a long box with $c > \sqrt{a^2 + b^2}$ has radius

$$\rho = \frac{1}{2} \sqrt{a^2 + b^2}. \quad (4)$$

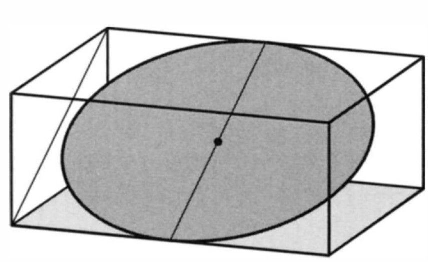


Figure 2 Largest wafer touching four sides

Short boxes Call an $a \times b \times c$ box with longest edge c *short* if $c \leq \sqrt{a^2+b^2}$. Our analysis of this case depends on a 1948 Putnam problem known as the "penny in a corner" problem [**9**]:

> *Penny in a corner.* Let ρ be a given positive real number. Find the locus of the center of a disk of radius ρ in the first octant that moves so as always to remain tangent to all three coordinate planes.

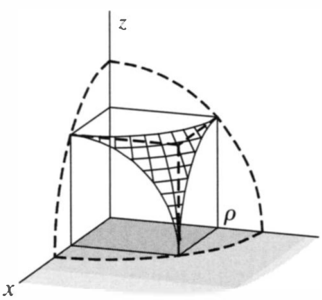


Figure 3 The locus of the center

The locus proves to be the portion Σ_ρ of the sphere of radius $\rho\sqrt{2}$ that lies in the cube with one vertex at the origin and the opposite vertex at the point (ρ, ρ, ρ), as shown in FIGURE 3. A proof can be found in Gleason et al. [**5**], but for the sake of completeness we sketch a somewhat simpler argument. Our reasoning depends on the following elementary result:

LEMMA 1. *Suppose a plane π with unit normal $\mathbf{n} = (l, m, n)$ passes though a point $P(p, q, r)$ and meets the coordinate xy-plane in a line w. Let Q be the foot of the perpendicular from P to w* (FIGURE 4). *Then*

$$r = \overline{PQ}\sqrt{1-n^2}. \tag{5}$$

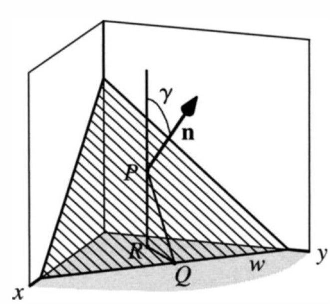


Figure 4 The key fact

Proof. Let R be the point $(p, q, 0)$, the foot of the perpendicular from P to the xy-plane, and let γ be the angle between the normal $\mathbf{n}$ and the z-axis, so that $n = \cos\gamma$. Since $\overrightarrow{QR}$, $\overrightarrow{QP}$, and $\mathbf{n}$ all lie in the plane perpendicular to w through P, we see that $\angle QPR = 90° - \gamma$, and so in right triangle PRQ, $r = \overline{PR} = \overline{PQ}\cos\angle QPR = \overline{PQ}\sin\gamma = \overline{PQ}\sqrt{1-n^2}$. ∎

Now suppose a wafer ω of radius ρ and center $P = (p, q, r)$ in the first octant is tangent to all three coordinate planes, let $\mathbf{n} = (l, m, n)$ be the *outward* normal of the plane π of the wafer, and assume initially that $lmn \neq 0$. Then π meets the coordinate planes $x = 0$, $y = 0$, and $z = 0$ in lines u, v, and w. The center P of ω is to be at distance ρ from each of these lines, and it follows from the lemma that P has coordinates

$$\left(\rho\sqrt{1-l^2}, \rho\sqrt{1-m^2}, \rho\sqrt{1-n^2}\right), \tag{6}$$

a formula that plainly holds even when $lmn = 0$. Solving for the normal shows that

$$\mathbf{n} = \left(\frac{1}{\rho}\sqrt{\rho^2 - p^2}, \frac{1}{\rho}\sqrt{\rho^2 - q^2}, \frac{1}{\rho}\sqrt{\rho^2 - r^2}\right). \tag{7}$$

The results claimed follow immediately:

LEMMA 2. (PENNY IN A CORNER) *Let ρ be a given positive real number. The locus of the center P of a disk of radius ρ in the first octant that is tangent to all three coordinate planes is the portion Σ_ρ of the sphere of radius $\rho\sqrt{2}$ centered at the origin that lies in the cube whose opposite corners are* (0, 0, 0) *and* (ρ, ρ, ρ) (FIGURE 3).

Proof. From (6) we see that P lies in the cube, and from (7) we conclude that $p^2 + q^2 + r^2 = 2\rho^2$ because $\mathbf{n}$ is a unit normal. Conversely, observe that if $P = (p, q, r)$ is any interior point of Σ_ρ and $\mathbf{n}$ is defined by (7), then the plane through P with normal $\mathbf{n}$ meets the coordinate planes in lines u, v, and w each of which is at distance ρ from P (Lemma 1). An analogous argument can be given at the boundary points of Σ_ρ. ■

We show next that a maximal centered wafer in a short box must touch all six faces of the box:

LEMMA 3. *If a centered wafer in a short box touches fewer than six faces of the box, then it is not maximal.*

Proof. The question is whether a centered wafer ω that touches just four faces of the box can be maximal. Suppose a centered wafer ω touches both $a \times c$ faces and both $b \times c$ faces of the box. The projection of ω into the $a \times b$ face is an ellipse—possibly degenerate—that touches all four edges of that face. The wafer itself lies in the right elliptic cylinder over that ellipse, and it has a diameter lying over, and parallel to, the major axis of that ellipse (FIGURE 5). If ω touches neither of the $a \times b$ faces, a suitable small rotation about that diameter (dashed in FIGURE 5) moves it so that it

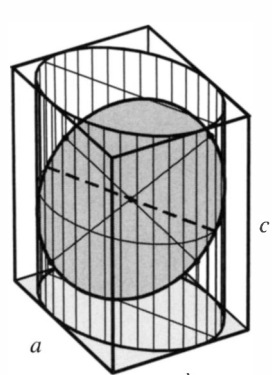


Figure 5 Proof of Lemma 3

has at most two points of contact with the box, showing that it is not maximal. (We thank one of the referees for suggesting this nice geometric argument.) ■

Finally, suppose the short $a \times b \times c$ box lies in coordinate 3-space $\mathbb{R}^3$ with one corner at the origin, the adjacent edges along the positive coordinate axes, and the opposite corner at the point (x, y, z), where (x, y, z) is a permutation of (a, b, c). Let ω be a centered wafer of radius ρ that lies in the box and touches all six faces of the box. Then, in particular, ω touches all three coordinate planes, so the center $S = \left(\frac{1}{2}x, \frac{1}{2}y, \frac{1}{2}z\right)$ of ω must lie on the surface Σ_ρ (according to Lemma 2). It follows that

$$\rho\sqrt{2} = \frac{1}{2}\sqrt{x^2 + y^2 + z^2} = \frac{1}{2}\sqrt{a^2 + b^2 + c^2},$$

and

$$\rho = \sqrt{\frac{a^2 + b^2 + c^2}{8}}. \tag{8}$$

This is the radius of the largest wafer that fits in the short box. Note that according to (7), the plane of the wafer whose radius is given by (8) has unit normal

$$\mathbf{n} = \left(\frac{\sqrt{-x^2 + y^2 + z^2}}{\sqrt{x^2 + y^2 + z^2}}, \frac{\sqrt{x^2 - y^2 + z^2}}{\sqrt{x^2 + y^2 + z^2}}, \frac{\sqrt{x^2 + y^2 - z^2}}{\sqrt{x^2 + y^2 + z^2}}\right). \tag{9}$$

Conclusions We summarize our results in the following theorem.

THEOREM. *The largest wafer that fits in an $a \times b \times c$ box with longest edge c has radius*

$$\rho_{\max} = \begin{cases} \frac{1}{2}\sqrt{a^2 + b^2} & \text{if } c > \sqrt{a^2 + b^2}, \\ \frac{1}{2}\sqrt{\frac{a^2 + b^2 + c^2}{2}} & \text{if } c \le \sqrt{a^2 + b^2}. \end{cases} \tag{10}$$

In the first case, there are infinitely many maximal wafers, exactly two of which are centered. In the second case, there are exactly four maximal wafers, and they are necessarily centered.

Proof. The result for a long box is (4). For a short box, exactly one maximum wafer, whose radius is given by (8), is associated with each of the four pairs of opposite vertices, as described above. ■

To rephrase, if a short box is placed with one corner at the origin and the opposite corner at (a, b, c), then the four unit normals are formed by choosing the signs $(+, +, +)$, $(-, +, +)$, $(+, -, +)$, and $(+, +, -)$ in

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

For example, the four maximal wafers in a $5 \times 7 \times 8$ box have radius $\frac{1}{2}\sqrt{69} \approx 4.15331$. Two of them are pictured in FIGURE 6; the other two are the mirror images of these in the horizontal medial plane.

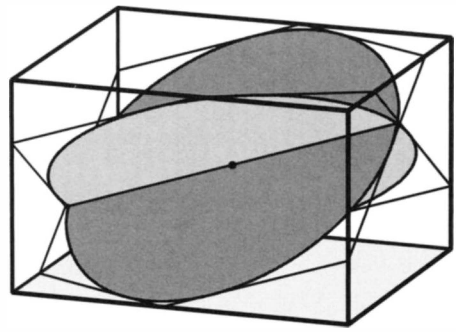


Figure 6 Two of the four maximal wafers

Concluding remarks The question of finding the radius of the largest disk that fits in a cube, or, more generally, in a box, has been around for a long time. For a cube it is well known that there are four such maximal disks, one inscribed in each of the cube's four regular-hexagonal cross-sections (see Shklarsky et al. [**10**]). For a box, the solution is more recent. Although we learned of it only after the present note was accepted for publication, the first published solution was apparently in 1998, when Everett et al. [**4**] considered the question already in $\mathbb{R}^d$.

Analogous notions in higher dimensions play an important role in problems in computer science and in mathematical programming. For a glimpse of this active area of research in computational geometry, see, for example, Gritzmann and Klee [**6**]. For each j with $1 \le j \le d$, a *j-ball* of *radius* ρ in $\mathbb{R}^d$ is a set geometrically congruent to

$$\left\{(x_1, x_2, \ldots, x_d) : \sum_{i=1}^{j} x_i^2 \le \rho^2 \quad \text{and} \quad x_i = 0 \quad \text{for} \quad j < i \le d\right\}$$

and a *j-cylinder* of *radius* ρ is a set geometrically congruent to

$$\left\{(x_1, x_2, \ldots, x_d) : \sum_{i=1}^{j} x_i^2 \le \rho^2 \quad \text{and} \quad -\infty < x_i < \infty \quad \text{for} \quad j < i \le d\right\}.$$

The *inner j-radius $r_j(K)$* of the convex body K is the largest radius of a j-ball that fits in K, and the *outer j-radius $R_j(K)$* is the smallest radius of a j-cylinder that contains K. Gritzmann and Klee, working more generally in Minkowski space, develop many basic algebraic and geometric properties of these radii, among them the following elegant duality: if K is a symmetric convex body and K^0 is its polar dual, then for each j,

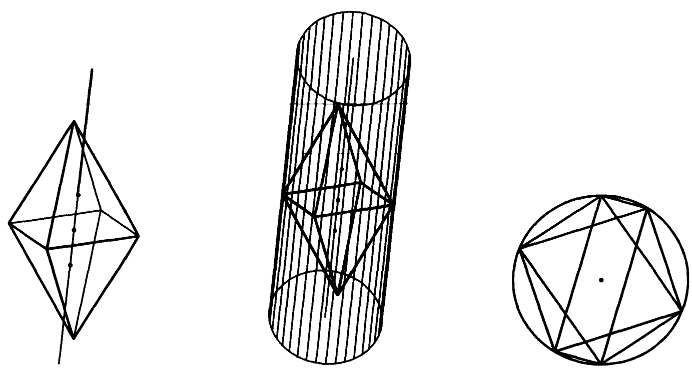
$$r_j(K) \cdot R_j\left(K^0\right) = 1. \tag{11}$$

(For a discussion of the polar dual, see, for example, Eggleston [**3**].) The inner and outer j-radii have been determined for many polytopes in $\mathbb{R}^d$. Brandenberg [**1**] provides an elaborate survey of what is known.

It is interesting to see what the duality (11) says for our $a \times b \times c$ box K in $\mathbb{R}^3$. The inner radius $r_2(K)$ is given in explicit terms by (10). The polar dual K^0 of the box K is the irregular octahedron with vertices $(\pm 2/a, 0, 0)$, $(0, \pm 2/b, 0)$, and $(0, 0, \pm 2/c)$; and according to (11) the radius of the smallest infinite circular cylinder that contains K^0 is the outer 2-radius $R_2(K) = 1/r_2(K) = 1/\rho_{\max}$.

For example, when K is the $5 \times 7 \times 8$ box pictured above in FIGURE 6, the polar dual K^0 of this box K is the irregular octahedron with vertices $(\pm 2/5, 0, 0)$,

$(0, \pm 2/7, 0)$, and $(0, 0, \pm 1/4)$, and the outer 2-radius $R_2(K^0)$ is $2/\sqrt{69}$. FIGURE 7 shows this octahedron and the smallest cylinder that contains it.



(a) The polar dual (b) Smallest cylinder (c) Axial view

Figure 7 The octahedron in the smallest cylinder

REFERENCES

1. René Brandenberg, Radii of regular polytopes, *Discrete Comput. Geom.*, to appear.
2. H. S. M. Coxeter and S. L. Greitzer, *Geometry Revisited*, New Mathematics Library 19, Random House and L. W. Singer, 1967.
3. H. G. Eggleston, *Convexity*, Cambridge Univ. Press, 1958.
4. H. Everett, I. Stojmenović, P. Valtr, and S. Whitesides, The largest k-ball in a d-dimensional box, *Comput. Geom.* **11** (1998), 59–67.
5. A. M. Gleason, R. E. Greenwood, and L. M. Kelly, *The William Lowell Putnam Mathematical Competition Problems and Solutions: 1938–1964,* Mathematical Association of America, 1980.
6. P. Gritzmann and V. Klee, Inner and outer j-radii of convex bodies in finite-dimensional normed spaces, *Discrete Comput. Geom.* **7** (1992), 255–280.
7. R. P. Jerrard, J. Schneider, R. Smallberg, and J. E. Wetzel, Straw in a box, preprint.
8. K. A. Post, Triangle in a triangle: On a problem of Steinhaus, *Geom. Dedicata* **45** (1993), 115–20.
9. G. W. Mackey, The William Lowell Putnam Mathematical Competition, *Amer. Math. Monthly* **55** (1948), 630–633.
10. D. O. Shklarsky, N. N. Chentzov, I. M. Yaglom, *Geometric Inequalities and Problems on Maxima and Minima* (in Russian), Nauka, Moscow, 1970.

A Theorem of Frobenius and Its Applications

DINESH KHURANA
Panjab University
Chandigarh-160014, India
dkhurana@pu.ac.in

ANJANA KHURANA
Punjabi University
Patiala (Punjab), India
an14in@yahoo.com

In any finite cyclic group, there are exactly d elements x satisfying $x^d = 1$ for each divisor d of its order. Consequently, in any finite abelian group, the number of solutions of $x^d = 1$ is a multiple of d, since we can write the group as a direct sum of cyclic groups. Remarkably, this result turns out to be true for *any* finite group. This is a fundamental theorem proved by Frobenius [**9**] more than hundred years ago, in 1895:

If d is a divisor of the order of a finite group G, then the number of solutions of $x^d = 1$ *in G is a multiple of d.*

This result (which we call *the Frobenius theorem*) has stimulated widespread interest in counting solutions of equations in groups; details can be found in Finkelstein [**8**]. Many proofs and generalizations of the result are known [**1**; **2**, p. 49; **3**, p. 92; **11**; **12**, p. 136; **18**, p. 77]. A standard proof (Frobenius's original one) is a consequence of the character theory of finite groups (see, for instance, Serre [**20**, Corollary 2, p. 83]), but now many elementary proofs are known. In spite of its fundamental nature, Frobenius's theorem, unlike the Sylow theorems, has not found its well-deserved place in undergraduate texts in algebra. In fact, even most of the recent graduate texts in group theory do not include the Frobenius theorem.

We present our own proof of the Frobenius theorem and some of its applications in a way that uses only elementary knowledge of group theory. For this purpose, we refer the reader to Herstein's book [**13**]. In the last section, we also discuss some applications of Frobenius's theorem to number theory.

Comparison with Sylow theory To show how useful the theorem may be, let us recall some standard results normally proved using the Sylow theorems in most undergraduate texts in algebra.

It is well known that every group of prime order is cyclic. Are there other natural numbers n such that, if G is a group of order n, then G is cyclic? Here is a typical approach using Sylow theory: Let $n = pq$, where $p < q$ are primes. The number of Sylow q-subgroups is $1 + kq$, for some k such that $1 + kq$ divides p. As $q > p$, $k = 0$ and so there is a unique subgroup of order q and which, therefore, is normal. If $p \nmid q - 1$, the subgroup of order p is also normal and G, being their direct sum, is cyclic. The Frobenius theorem gives a stronger result, allowing us to characterize all such values of n. These turn out to be precisely those n for which n and $\phi(n)$ are relatively prime (where $\phi(n)$ is the number of positive integers less than n that are relatively prime to n).

A group G is called *simple* if its only normal subgroups are G and $\{1\}$. For instance, abelian simple groups are just the cyclic groups of prime order. A group is said to be *solvable* if it contains a sequence of normal subgroups $\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd G$ such that each quotient N_{j+1}/N_j is abelian. In particular, a solvable nonabelian group is not simple.

As noted above, in a group G of order pq, where $p < q$ are primes, the Sylow q-subgroup is normal and thus G is not simple. With a little more effort the Sylow theory shows that the Sylow r-subgroup is normal in a group of order pqr, where $p < q < r$ are primes. But Sylow theorems do not work for this purpose if the order of the group is a product of more than three distinct primes. Using the Frobenius theorem, it can be easily proved that if every Sylow p-subgroup of G is cyclic (for instance, if the order of the group is squarefree) and q is the largest prime divisor of the order of group, then the Sylow q-subgroup is normal and thus G is not simple. Burnside [**2**, p. 503] remarked, "... simple (nonabelian) groups of odd order do not exist." His claim was proved in 1963 by Feit and Thompson [**7**] when they showed that every group of odd order is solvable. Indeed, if G is a nonabelian group of odd order, then the commutator subgroup G' is a proper normal subgroup showing that G is not simple.

Using the Frobenius theorem, one can easily prove that a group, all of whose Sylow subgroups are cyclic, is solvable.

The Frobenius Theorem Throughout, G denotes a finite group and $o(g)$ the order of $g \in G$. By $|S|$, we mean the number of elements in a finite set S. By $H \leq G$ (resp. $H \trianglelefteq G$) we mean that H is a subgroup (normal subgroup) of G. If d divides $|G|$, then

$$A_d = \{x \in G : x^d = 1\}.$$

If $S \subseteq G$, then $\langle S \rangle$ will denote the subgroup of G generated by S. We denote the greatest common divisor and least common multiple of m and n by $\gcd(m, n)$ and $\text{lcm}(m, n)$, respectively. For an element $a \in G$, $N(a) = \{g \in G : ag = ga\}$ is the *centralizer* of a and $C(a) = \{gag^{-1} : g \in G\}$ is the conjugacy class of a. We begin with the following lemma, which we shall use repeatedly in the paper.

LEMMA. *For any n, the number of elements of order n in G is either* 0 *or a nonzero multiple of $\phi(n)$. Furthermore, if a divisor of $|G|$ has the form $d = p^\alpha s$, where $p^{\alpha+1}$ divides $|G|$ and* $\gcd(p, s) = 1$, *then the set $A = A_{dp} \backslash A_d$ is either empty or has cardinality a multiple of $\phi(p^{\alpha+1})$.*

Proof. We define a relation on the elements of G as follows: x is related to y if and only if they generate the same subgroup, that is, $\langle x \rangle = \langle y \rangle$. Clearly this is an equivalence relation. As $o(x) = o(x^t)$ if and only if $\gcd(t, o(x)) = 1$, the equivalence class of x has $\phi(o(x))$ elements. Writing G as a disjoint union of its equivalence classes, it follows that the set of elements of a given order n is a union of equivalence classes and, thus, its cardinality is a multiple of $\phi(n)$.

To prove the second statement, we note that the set A can also be written as $\{x : o(x) = p^{\alpha+1}s_1,\ s_1 \mid s\}$. If $A \neq \emptyset$, then it is a union of equivalence classes and the equivalence class of any element x with $o(x) = p^{\alpha+1}s_1$ has cardinality a multiple of $\phi(p^{\alpha+1})$, since $\phi(p^{\alpha+1}s_1) = \phi(p^{\alpha+1})\phi(s_1)$. It follows that $|A|$ has cardinality a multiple of $\phi(p^{\alpha+1})$. ■

We recall one well-known fact before proving the Frobenius theorem. This is:

If $x \in G$ has $o(x) = mn$, where $\gcd(m, n) = 1$, *then $x = yz$ for some y, z in G with $o(y) = m$, $o(z) = n$, and $yz = zy$.*

(Hint for proof: Find integers a and b with $am + bn = 1$. Set $y = x^{bn}$, etc.)

THEOREM. (FROBENIUS) *If d divides $|G|$ then d divides $|A_d|$.*

Proof. We proceed by double induction on $|G|$ and d. Note that the induction is started trivially with $|G| = d = 1$. Assume $|G| > 1$ and $d < |G|$ (since the case $d = |G|$ is evident) and, that the result holds for larger divisors of $|G|$ and groups with order $< |G|$.

Let p be any prime divisor of $|G|/d$ and let $d = p^\alpha s$, where $\gcd(p, s) = 1$. Let $A = A_{dp} \backslash A_d$. Note that $|A_{dp}| = |A_d| + |A|$ and as d divides $|A_{dp}|$ (by the induction hypothesis), it is enough to show that d divides $|A|$. If $A = \emptyset$, then we are through, so we assume that $A \neq \emptyset$. By the lemma, $|A|$ is a multiple of $\phi(p^{\alpha+1}) = p^\alpha(p - 1)$. Thus we only have to show that s divides $|A|$.

Since $A = \{x : o(x) = p^{\alpha+1}s_1,\ s_1 \mid s\}$, the fact noted above shows that every element x of A has the form $yz = zy$, where $o(y) = p^{\alpha+1}$ and $z^s = 1$.

For $a \in G$ of order $p^{\alpha+1}$, let us define $S_a = \{ab : b \in N(a) \text{ and } b^s = 1\}$. Define $S_{C(a)} = \cup\{S_x : x \in C(a)\}$. Then A is a union of the sets S_a. We now show that the union is disjoint. Let $o(a) = o(a_1) = p^{\alpha+1}$ and $ab = a_1b_1$ with $b^s = b_1^s = 1$, where $ab = ba$ and $a_1b_1 = b_1a_1$. Note that $(ab)^s = (a_1b_1)^s$ implies that $a^s = a_1^s$. Since

$a^{p^{\alpha+1}} = a_1^{p^{\alpha+1}}$ and $\gcd(p^{\alpha+1}, s) = 1$, we have $a = a_1$ showing that A is a *disjoint* union of the sets S_a. So it is enough to show that s divides $|S_{C(a)}|$.

Note that $ab \to xax^{-1}xbx^{-1}$ is a bijection from $S_a \to S_{xax^{-1}}$. Thus $|S_{C(a)}| = |C(a)||S_a|$. Let $o(N(a)/\langle a\rangle) = k$ and $m = \gcd(s, k)$. Then $ab \to b\langle a\rangle$ is a bijection from

$$S_a \to \{y \in N(a)/\langle a\rangle : y^s = 1\} = \{y \in N(a)/\langle a\rangle : y^m = 1\}.$$

As $|N(a)/\langle a\rangle| < |G|$, the induction hypothesis implies that

$$\left|\{y \in N(a)/\langle a\rangle : y^m = 1\}\right| = |S_a| = cm \quad \text{for some natural number } c.$$

Also $|S_{C(a)}| = |C(a)||S_a| = |G||S_a|/|N(a)| = |G|cm/kp^{\alpha+1}$. Since both k and s divide $|G|$, so does $\operatorname{lcm}(k, s) = ks/m$, showing that s divides $|G|cm/k$. Finally, as $p^{\alpha+1}$ divides $|G|cm/k$ and $\gcd(p, s) = 1$, we see that s divides $|S_{C(a)}|$. ∎

Some applications in group theory In this section, we give some group-theoretic applications of the Frobenius theorem, including those stated in the introduction. We shall tacitly use the following fact: *If d divides $|G|$ and $|A_d| = d$, then any subgroup H of order d coincides with A_d and is thus normal in G.*

APPLICATION 1. *Let $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1 < p_2 < \cdots < p_r$ are primes. If every Sylow p-subgroup of G is cyclic, then a Sylow p_r-subgroup is normal in G (and is thus unique). Moreover, G is solvable. In particular, if $|G|$ is squarefree and p is the largest prime divisor of $|G|$, then the Sylow p-subgroup is normal in G and G is solvable.*

Proof. We show that $|A_d| = d$ for every divisor d of $|G|$ that can be written in a particular form, namely $d = p_k^{\beta_k} p_{k+1}^{\alpha_{k+1}} \dots p_r^{\alpha_r}$, $1 \le k \le r$ and $\beta_k \le \alpha_k$. We proceed by induction on d. For $d = |G|$, the result follows trivially. Assume $d < |G|$ and that the result holds for larger divisors of the given type. Let p be the largest prime divisor of $|G|/d$ and $A = A_{dp} \setminus A_d$. As a Sylow p-subgroup is cyclic, $A \neq \emptyset$. By our assumption, $|A_{dp}| = dp$ and by the Frobenius theorem, $|A_d| = dt$ for some $1 \le t < p$. By the lemma, $p - 1$ divides $dp - dt = d(p - t)$. As every prime divisor of d is greater than or equal to p, $\gcd(p - 1, d) = 1$ and so $p - 1 | p - t$, implying that $t = 1$. Thus $|A_d| = d$ and, in particular, $|A_{p_r^{\alpha_r}}| = p_r^{\alpha_r}$ implying that a Sylow p_r-subgroup N is normal. Now by induction on the size of the group, N and G/N are solvable and thus G is solvable.

As every group of prime order is cyclic, the "in particular" part is now clear. ∎

APPLICATION 2. *Let n be a positive integer. Then every group of order n is cyclic if and only if* $\gcd(n, \phi(n)) = 1$.

Proof. One can easily check that $\gcd(n, \phi(n)) = 1$ if and only if n is squarefree and $p \nmid q - 1$, where p and q are prime divisors of n.

Necessity We exhibit a noncyclic group for each n where $\gcd(n, \phi(n)) \neq 1$. If $p^2 \mid n$, for some prime p, then $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{n/p^2}$ is a noncyclic group of order n (recall that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$). Now suppose n is squarefree and $p < q$ are two prime divisors of n such that $p \mid q - 1$. As $\mathbb{Z}_q \setminus \{0\}$ is group under multiplication modulo q and $p \mid q - 1$, there exists a subgroup, say H, of order p. Define an operation on elements of $\mathbb{Z}_q \times H$ by $(x, h)(y, k) = (x + hy, hk)$. Then $\mathbb{Z}_q \times H$ is a group with identity (0, 1) in which $(x, h)^{-1} = (-h^{-1}x, h^{-1})$. Note that if $h \neq 1$, then $(1, h)(1, 1) \neq (1, 1)(1, h)$ showing that $G = \mathbb{Z}_q \times H$ is nonabelian. Thus $G \times \mathbb{Z}_{n/pq}$ is a nonabelian group of order n.

Sufficiency We show that $|A_d| = d$ for every divisor d of $|G|$. We proceed by induction on d. For $d = |G|$, the result follows trivially. Assume $d < |G|$ and that the result holds for all divisors greater than d. Let p be any prime divisor of $|G|/d$ and $A = A_{dp} \backslash A_d$. Clearly $A \neq \phi$. By our assumption, $|A_{dp}| = dp$ and by the theorem, $|A_d| = dt$ for some $1 \leq t < p$. Arguing just as in Application 1, we see that that $t = 1$ and so $|A_d| = d$. In particular, $|A_p| = p$ for every prime divisor of $|G|$, which implies that every Sylow p-subgroup is normal. Thus G, being direct sum of its cyclic Sylow p-subgroups of co-prime order, is cyclic. ■

Dickson [**6**] characterized $n \in \mathbb{N}$ such that every group of order n is abelian. Miller and Moreno [**17**] studied nonabelian groups in which every subgroup is abelian. They proved that the order of a nonabelian group whose every proper subgroup is abelian can have at most two distinct prime factors.

As already mentioned, if $|A_d| = d$, then every subgroup of order d coincides with A_d and is thus normal. But the converse is not true; a normal subgroup of order d may not coincide with A_d. For example, if $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $N = \langle(1, 0)\rangle$, then $N \trianglelefteq G$ and $|N| = 2$, but $|A_2| = 4$. But if $N \trianglelefteq G$ and $\gcd(|N|, |G/N|) = 1$, then $N = A_{|N|}$. To see this let $a \in A_{|N|}$. Now $aN \in G/N$ implies $a^{|G/N|} \in N$ and $a \in A_{|N|}$ implies $a^{|N|} = 1 \in N$. This, in light of $\gcd(|N|, |G/N|) = 1$, implies that $a \in N$.

A similar argument shows that if $K \trianglelefteq N \trianglelefteq G$ with $\gcd(|K|, |N|/|K|) = 1$, then $K \trianglelefteq G$. For if $k \in K$ and $g \in G$, then $x = gkg^{-1} \in N$. Thus $x^{|N/K|} \in K$ and $x^{|K|} = 1 \in K \Rightarrow x \in K$. But this is not true for any chain of normal subgroups. For example, if we take $G = A_4$, $N = V_4 = \{I, (12)(34), (13)(24), (23)(14)\}$, and $K = \{I, (12)(34)\}$, then $K \trianglelefteq N \trianglelefteq G$ but K is not normal in G. What went wrong here is the fact that $\gcd(|K|, |N/K|) \neq 1$.

In 1895, Frobenius conjectured (in the same paper where he proved the theorem that bears his name [**9**]) that if $|A_d| = d$, then A_d forms a subgroup. The work of many group theorists went into proving the conjecture. Its final proof was announced in 1991 [**14**] and the details appeared later [**15**].

Let $|G| = p^\alpha m$, where p is the smallest prime divisor of $|G|$ and $\gcd(p, m) = 1$. If the Sylow p-subgroup is cyclic, then, as argued in Application 1, $|A_{n/p^\beta}| = n/p^\beta$, for all $1 \leq \beta \leq \alpha$. Thus, it follows from Frobenius's conjecture that G has subgroups of order n/p^β, for all $1 \leq \beta \leq \alpha$.

Some applications in number theory Many authors have studied A_d in symmetric groups [**4, 5, 16, 19**]. It is well known that two elements in S_n are conjugate if and only if they have the same cyclic decomposition [**13**, p. 88]. So if the cyclic decomposition of $\sigma \in S_n$ into m cycles has n_i cycles of length l_i with $l_i \geq 1$ and $\sum_i l_i n_i = n$, then one can show that the size of the conjugacy class of σ in S_n is

$$n! \Big/ \prod_{i=1}^{m} l_i^{n_i} \prod_{i=1}^{m} n_i! \tag{1}$$

and that the number of r-cycles in S_n is $n!/r(n-r)!$. The Frobenius theorem gives us many useful number-theoretic identities just by finding suitable $|A_d|$ for appropriate values of d in symmetric groups.

APPLICATION 3. *For any prime p and any natural number $n \geq p$, we have*

$$\sum_{k=1}^{t} \frac{n!}{p^k (n-kp)!\,k!} \equiv -1 \pmod{p},$$

where t is the largest natural number such that $tp \leq n$.

Proof. As A_p in S_n contains only those elements that are products of p-cycles and 1-cycles (fixed points), then by equation (1)

$$|A_p| = 1 + \sum_{k=1}^{t} \frac{n!}{p^k(n-kp)!\,k!},$$

where the summand counts those permutations that are the product of k p-cycles and $n - kp$ fixed points, and the initial 1 counts the identity permutation. Thus, the result follows from the Frobenius theorem. ∎

Note that by putting $n = p$ in Application 3, we get Wilson's theorem (that is, $(p-1)! \equiv -1 \pmod{p}$ for any prime p).

APPLICATION 4. *If $n/2 < p_1 < p_2 < \cdots < p_k \leq n$, where $n \in \mathbb{N}$ and each p_i is prime, then*

$$\sum_{t=1}^{k} \frac{n!}{p_t(n-p_t)!} \equiv -1 \pmod{p_1 p_2 \ldots p_k}.$$

Proof. Find $|A_{p_1 p_2 \cdots p_k}|$ in S_n as in Application 3 above. ∎

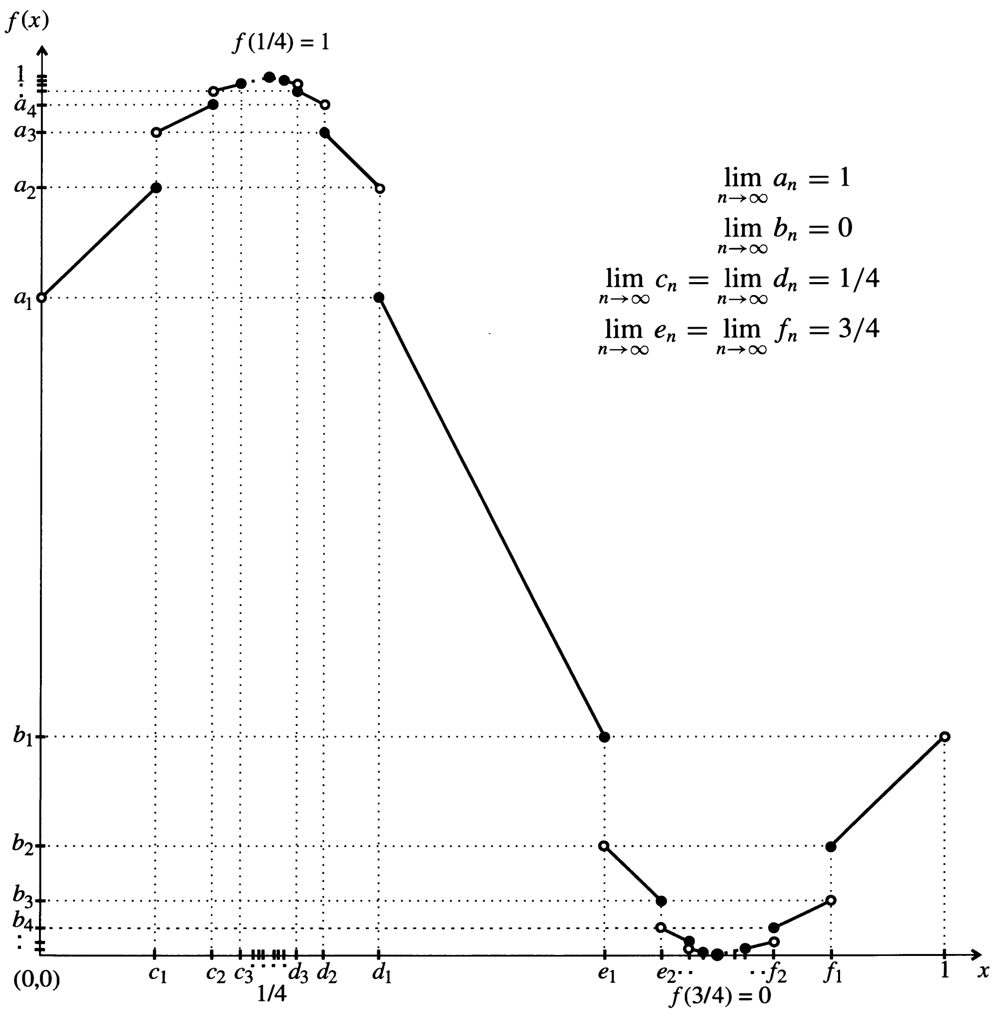
Proceeding along the same lines one may obtain many such identities.

Acknowledgment. We thank Professor Bhandari and Professor Gupta for some useful discussions. We are highly indebted to Professor B. Sury for many suggestions to improve the quality of the paper. Thanks are also due to the referees for their helpful comments.

REFERENCES

→ R. Brauer, On a theorem of Frobenius, *Amer. Math. Monthly* **76** (1969), 12–15.
2. W. Burnside, *The Theory of Groups of Finite Order*, 2nd ed., Dover, New York, 1955.
3. R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Dover, New York, 1956.
4. S. Chowla, I. N. Herstein, and W. K. Moore, On recursions connected with symmetric groups I, *Canad. J. Math.* **3** (1951), 328–334.
5. S. Chowla, I. N. Herstein, and W. R. Scott, The solutions of $X^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh. (Trondheim)* **25** (1952), 29–31.
6. L. E. Dickson, Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.* **6** (1905), 198–204.
7. W. Feit and J. G. Thompson, Solvability of groups of odd orders, *Pacific J. Math.* **13** (1963), 775–1029.
8. H. Finkelstein, Solving Equations in groups, *Period. Math. Hungar.* **9** (1978), 187–204.
9. F. G. Frobenius, Verallgemeinerung des Sylowschen Satzes, *Berliner Sitz.* (1895), 981–993.
10. ———, Über endliche gruppen, *Berliner Sitz.* (1895), 81–112.
11. ———, Über einen Fundamentalsatz der Gruppentheorie, *Berliner Sitz.* (1903), 987–991.
12. M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.
13. I. N. Herstein, *Topics in Algebra*, Blaisdell, New York, 1964.
14. N. Iiyori and H. Yamaki, On a conjecture of Frobenius, *Bull. Amer. Math. Soc.* **25** (1991), 413–416.
15. N. Iiyori, A conjecture of Frobenius and the simple groups of Lie type IV, *J. Algebra* **154** (1993), 188–214.
16. E. Jacobstal, Sur le nombre d'éléments du groupe symétrique S_n dont l'ordre est un nombre premier, *Norske Vid. Selsk. Forh. (Trondheim)* **21** (1949), 49–51.
→ G. A. Miller and H. C. Moreno, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.* **4** (1903), 398–404.
18. G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and Application of Finite Groups*, Dover, New York, 1961.
19. L. Moser and M. Wyman, On solutions of $X^d = 1$ in symmetric groups, *Canad. J. Math.* **7** (1955), 159–168.
20. J. P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag GTM **42**, 1997.

Proof Without Words: (0, 1) and [0, 1] Have the Same Cardinality



—KEVIN HUGHES AND TODD K. PELLETIER
ROWAN UNIVERSITY
GLASSBORO, NJ 08028

A "Base" Count of the Rationals

BRIAN D. GINSBERG
375 Riverside Dr., Room 5AA
New York, NY 10025
bginsb@law.columbia.edu

In 1874, Cantor showed that the set of rational numbers $\mathbb{Q}$ is countable—that is, equipotent to the set of natural numbers $\mathbb{N}$—by arranging its elements in a grid and sweeping out paths of ever-increasing length, numbering elements as they are traversed [**1**]. Here, we present a new way to do this, which relies instead on constructing a couple of simple functions.

Counting $\mathbb{Q}$ Consider a base-12 number system with / as the symbol for the digit 10 and $-$ as the symbol for 11. Define the map $\varphi\colon \mathbb{Q} \to \mathbb{N}_{(12)}$ (the natural numbers written in base-12) by $\varphi(a/b) = a/b$, where, on the left-hand side, a/b is the lowest-terms representation of a typical element of $\mathbb{Q}$ and, on the right-hand side, a/b means the base-12 number consisting of the digits of a (possibly preceded by a minus sign $-$), followed by the division slash / and then the digits of b.

For example, $\varphi(-5/12) = -5/12$. Let $\sigma\colon \mathbb{N}_{(12)} \to \mathbb{N}$ be the obvious injection converting a number from base-12 to base-10. Continuing our example, this means

$$\sigma(-5/12) = 11 \cdot 12^4 + 5 \cdot 12^3 + 10 \cdot 12^2 + 1 \cdot 12^1 + 2 \cdot 12^0 = 238{,}190.$$

Then $\sigma \circ \varphi\colon \mathbb{Q} \to \mathbb{N}$ is an injection, whereby $|\mathbb{Q}| \leq |\mathbb{N}|$. Inclusion provides the reverse inequality, and we conclude $|\mathbb{Q}| = |\mathbb{N}|$.

Counting $\mathbb{A}$ The set $\mathbb{A}$, called the *algebraic numbers*, is the set of all numbers, possibly complex, that are roots of some monic polynomial with rational coefficients [**2**]. For example, $\sqrt{2}$ and $3i$ are algebraic numbers—roots of $x^2 - 2$ and $x^2 + 9$, respectively—whereas π and e are not. It turns out that we can count $\mathbb{A}$ using the same technique we used to count $\mathbb{Q}$. Namely, find an injection from $\mathbb{A}$ into $\mathbb{N}$ and then use inclusion to get equipotentiality.

Proceeding in this way, observe that given $\alpha \in \mathbb{A}$, there exists a unique monic polynomial P_α of smallest degree n given by

$$P_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

where $a_j \in \mathbb{Q}$, such that α is a root of P_α and P_α has no repeated roots. Therefore P_α has n roots $r_1, \ldots, r_n$, all distinct.

Write r_j in polar coordinates as $\rho_j e^{i\theta_j}$, where $0 \leq \rho_j < \infty$ and $0 \leq \theta_j < 2\pi$, and define the total ordering $\prec$ on the set of roots of P_α as follows: $r_j \prec r_k$ if and only if $\rho_j < \rho_k$ or $\rho_j = \rho_k$ and $\theta_j < \theta_k$. Use $\prec$ to re-label the roots such that $r_1 \prec \cdots \prec r_n$. Then α is uniquely described by the coefficients $a_{n-1}, \ldots, a_0$ and the position j (as a root of P_α) of α, where $1 \leq j \leq n$, when ordered by $\prec$ as a root of P_α.

Add the comma , to our existing 12-symbol alphabet and consider the map $\psi\colon \mathbb{A} \to \mathbb{N}_{(13)}$ defined by $\psi(\alpha) = a_{n-1}, \ldots, a_0, j$ (a sort of concatenation of the sequence of coefficients followed by the position j of α). Let $\tau\colon \mathbb{N}_{(13)} \to \mathbb{N}$ be the obvious injection converting a number from base-13 to base-10. Then $\tau \circ \psi\colon \mathbb{A} \to \mathbb{N}$ is an injection, so $|\mathbb{A}| \leq |\mathbb{N}|$. Inclusion gives the reverse inequality, and we see that $\mathbb{A}$ is countable.

Conclusion This method of enumerating sets certainly does not displace Cantor's classic technique, but it does show another, more concrete way to accomplish the task. Though we applied it only to $\mathbb{Q}$ and $\mathbb{A}$, the method presented here can, in theory, be used to count any set X such that $\mathbb{N} \subseteq X$ (so that we may apply inclusion) for which a sufficiently clever function from X into $\mathbb{N}_{(n)}$ for some n can be found.

Acknowledgment. This work was supported by the Paul K. and Evalyn E. Cook Richter Memorial Trust, while the author was simultaneously pursuing a B.S. and M.S. in mathematics at Yale University.

REFERENCES

1. Georg Cantor, Ueber eine Eigenschaft des Inbergriffs aller reellen algebraischen Zahlen, *J. f. Math.* **77** (1874), 258–262.
2. I. N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley & Sons, New York, 1975, 214–219.

Covering Systems of Congruences

J. FABRYKOWSKI
T. SMOTZER
Youngstown State University
Youngstown, Ohio 44555
jfabryk@math.ysu.edu
tsmotzer@math.ysu.edu

Let us consider the following problem, which is a variant of problem 9 from the 2002 American Invitational Mathematics Examination (AIME):

PROBLEM. Harold, Tanya, and Ulysses paint a very long fence. Harold starts with the first picket and paints every hth picket; Tanya starts with the second picket and paints every tth picket; and Ulysses starts with the third picket and paints every uth picket. If every picket gets painted exactly once, find all possible triples (h, t, u).

Solution: Label the pickets 1, 2, 3, and so on. Ulysses cannot paint picket 4 or else Ulysses paints all the pickets thereafter. Suppose Harold paints picket 4. Then Ulysses cannot paint picket 5, or else Harold and Ulysses both paint picket 7, so Tanya paints picket 5. Ulysses paints picket 6 and $(h, t, u) = (3, 3, 3)$. On the other hand, suppose Tanya paints picket 4. Then Ulysses cannot paint picket 5, or else there is nothing left for Harold to paint, so Harold paints picket 5. Hence Ulysses paints picket 7 and $(h, t, u) = (4, 2, 4)$.

This problem really asks about how one can partition the set of integers into three arithmetic progressions. The second triple $(4, 2, 4)$ is a bit more interesting than the first, since not all the differences are equal. In elementary number theory, arithmetic progressions are equivalently called residue classes of various moduli. In such a setting, the arithmetic progression $a + km$, $k \in \mathbb{Z}$ is denoted by $a \pmod{m}$.

One can generalize the AIME problem and ask whether there exists a finite set of congruences, with all moduli distinct and greater than or equal to 2, that forms a partition of the set of integers. This turns out to be impossible [**4**]. Relaxing the assumption about *partitioning* the integers, one can look for finite sets of congruences such that every integer belongs to *at least one* of them.

Our purpose in this note is to survey this topic and provide an elementary proof of the relationship between two well-known conjectures.

Erdős's covering systems In 1849, A. de Polignac conjectured that any odd integer $n \geq 3$ can be expressed in the form $2^k + p$, where k is a nonnegative integer and p is either a prime or the integer 1 [**6**]. In 1950, Erdős refuted this by proving that there exists an arithmetic progression, no term of which has the given form.

To prove his assertion, Erdős developed the concept of *covering systems of congruences*. A family of residue classes $a_i \pmod{n_i}$ with $2 \leq n_1 \leq \cdots \leq n_r$ is called a covering system of congruences if every integer belongs to at least one of the residue classes, that is, every integer satisfies at least one of the congruences $x = a_i \pmod{n_i}$.

This is how Erdős's proof worked: Consider the system of congruences (which can be shown to be a covering system): $0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $3 \pmod 8$, $7 \pmod{12}$, and $23 \pmod{24}$ [**2, 3**]. Each of these congruences implies a corresponding congruence for certain powers of 2. For example, the congruence $k \equiv 1 \pmod 4$ together with $2^4 \equiv 1 \pmod 5$ imply that $2^k \equiv 2 \pmod 5$. To see this, let $k = 4n + 1$ and observe that

$$2^k \equiv 2^{4n+1} \equiv 2(2^4)^n \equiv 2 \pmod 5.$$

By similar reasoning, if k is a nonnegative integer, then at least one of the following congruences holds: $2^k \equiv 1 \pmod 3$, $2^k \equiv 1 \pmod 7$, $2^k \equiv 2 \pmod 5$, $2^k \equiv 8 \pmod{17}$, $2^k \equiv 2^7 \pmod{13}$, or $2^k \equiv 2^{23} \pmod{241}$.

Now consider the congruences $1 \pmod 3$, $1 \pmod 7$, $2 \pmod 5$, $8 \pmod{17}$, $2^7 \pmod{13}$, and $2^{23} \pmod{241}$. Since the moduli are pairwise relatively prime, there are infinitely many integers that satisfy all the congruences, by virtue of the Chinese Remainder Theorem. Now, if an odd integer a satisfies all the congruences, then all the integers of the form $a - 2^k$ are divisible by one of the moduli 3, 7, 5, 17, 13 or 241. It follows that $a - 2^k$ is not prime and therefore a does not have the form $2^k + p$.

Another example of application of covering systems of congruences came from R. L. Graham [**5**]. His result is in a sense opposite to a well-known conjecture stating that the Fibonacci sequence, defined by $f_0 = 0$, $f_1 = 1$, and for $n \geq 0$ $f_{n+2} = f_{n+1} + f_n$, contains infinitely many primes. Graham used covering systems to show that one can choose the initial relatively prime values f_0 and f_1 so that the corresponding sequence contains only composite integers. The smallest known choice is

$$f_0 = 331635635998274737472200656430763$$

and

$$f_1 = 1510028911088401971189590305498785.$$

The major open problem in this topic is a conjecture of Erdős, that for every $c \geq 2$ there is a covering system of congruences with $n_1 \geq c$ and distinct moduli. This is known to be true for some values of c; the current record, held by Choi [**1**], is $c = 20$. If there is a covering system of congruences with distinct moduli, and $n_1 \geq c$ for every $c \geq 2$, then one would obtain the following result about arithmetic progressions: For every positive integer m there exists an arithmetic progression, no term of which is a sum of a power of two and an integer, having at most m prime factors [**4**].

Two other important conjectures are by Selfridge and Schinzel:

SELFRIDGE CONJECTURE. There is no covering system of congruences with distinct odd moduli.

SCHINZEL CONJECTURE. In every covering system $a_i \pmod{n_i}$ with $1 \leq i \leq r$, there exists $i \neq j$ such that $n_i \mid n_j$.

Schinzel has proved that Selfridge's conjecture implies the Schinzel conjecture using the irreduciblity of certain polynomials [**7**]. We propose to prove this result using only elementary methods.

Main result We begin with a definition. Let $a_s \pmod{n_s}$ with $1 \leq s \leq r$ be a covering system of congruences. Then it is a *reduced covering system of congruences* if no proper subset of the covering system of congruences is a covering system of congruences.

THEOREM. *The Selfridge conjecture implies the Schinzel conjecture.*

Proof. Let us assume that the Selfridge conjecture holds, but the Schinzel conjecture does not. Then there is a reduced system of covering congruences, $a_s \pmod{m_s}$, such that $m_i \nmid m_j$ for all $i \neq j$. Let $m_i = 2^{\beta_i} O_i$, where O_i is odd for $1 \leq i \leq r$. Let us also assume that the congruences have been numbered in such a way that if $i < j$ then $\beta_i \leq \beta_j$. It follows from the Selfridge conjecture that $\beta_r > 0$. Obviously, all the numbers O_i are different.

Now, if $O_i \geq 3$ for all i, then we would contradict the Selfridge conjecture since if $x \equiv a_i \pmod{2^{\beta_i} O_i}$, and $2^{\beta_i} \mid (2^{\beta_i} O_i)$, then $x \equiv a_i \pmod{O_i}$, and we would have a covering system with all odd moduli. Consequently, if $a_i \pmod{m_i}$ is a covering system of congruences and $n_i | m_i$ for each i, then $a_i \pmod{n_i}$ is also a covering system of congruences. Thus, there exists i_0, such that $O_{i_0} = 1$ and consequently $m_{i_0} = 2^{i_0}$. It follows that $i_0 = r$ or else we would have $m_{i_0} \mid m_{i_0+1}$.

Next, we shift the system of congruences by $-a_r$, that is, change the variable x to $x + a_r$, so that we may assume that the rth congruence has the form $0 \pmod{2^{\beta_r}}$. Consider now integers of the form $x2^{\beta_r} - 1$, with $x \in \mathbb{Z}$. None of these integers is covered by the congruence $0 \pmod{2^{\beta_r}}$, however all of them are covered by the rest of the congruences, since the system is a covering system. Our system now takes the form:

$$x2^{\beta_r} - 1 \equiv a_s \pmod{m_s} \quad 1 \leq s \leq r-1. \tag{*}$$

Note that it may happen that not all of the congruences have solutions; however, whenever a congruence has solutions, we must have

$$\gcd(2^{\beta_r}, m_s) \mid a_s + 1.$$

Since $\gcd(2^{\beta_r}, m_s) = 2^{\beta_s}$, it follows that $2^{\beta_s} \mid a_s + 1$. Let

$$U = \{s : 1 \leq s \leq r-1 \quad \text{such that} \quad 2^{\beta_s} \mid a_s + 1\}.$$

For every $s \in U$, the congruence (*) takes the form $x2^{\beta_r - \beta_s} \equiv (a_s + 1)/2^{\beta_s} \pmod{O_s}$ or $x \equiv c_s \pmod{O_s}$ for some integers c_s. This new system of congruences is a covering system of congruences with all distinct odd moduli, contradicting the Selfridge conjecture. ∎

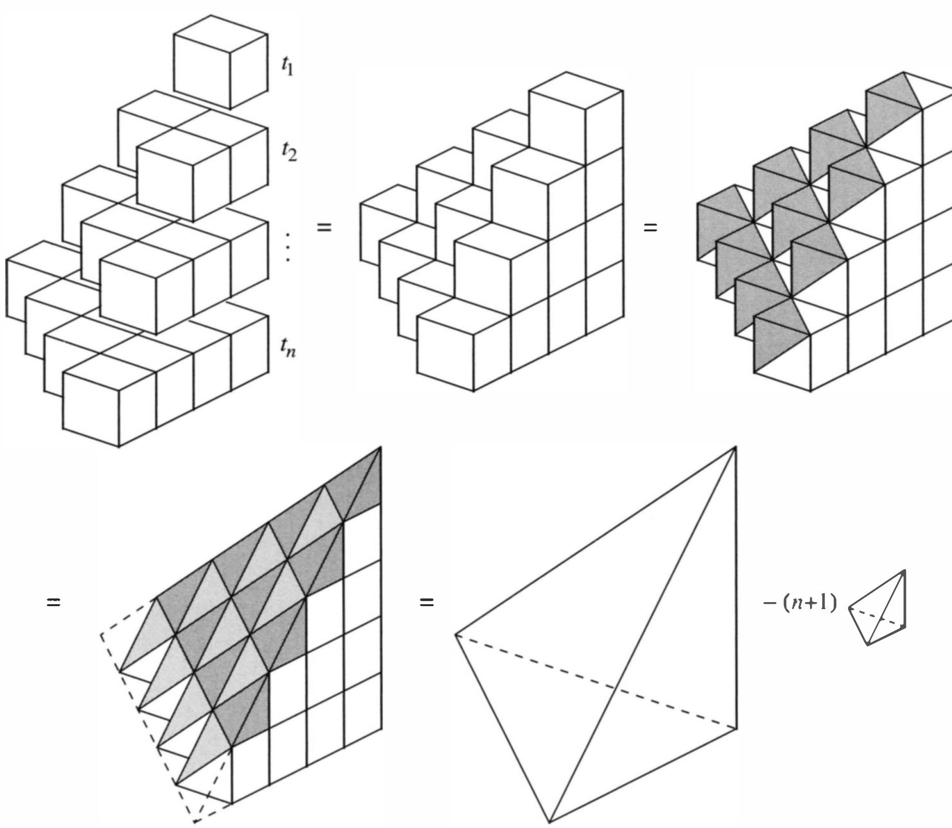
REFERENCES

1. S. Choi, Covering the set of integers by congruence classes of distinct moduli, *Math. Comp.* **25** (1971), 885–895.
2. P. Erdős, On integers of the form $2^n + p$ and some related problems, *Summa Brasil Math.* **11** (1950), 1–11.
3. ———, On a problem concerning congruence systems, *Mat. Lapok* **3** (1952), 122–128.
4. P. Erdős and R. L. Graham, Old and new problems and results in combinatorial number theory, *Monogr. Enseign Math.* **28**, L'Enseignement Mathématique, Geneva, 1980.
5. R. L. Graham, A Fibonacci-like sequence of composite numbers, this MAGAZINE **37** (1964), 322–324.

6. A. de Polignac, Six propositions arithmologiques déduites du crible d'Eratosthene, *Nouv. Ann. Math.* **8** (1849), 423–429.
7. A. Schinzel, Reducibility of polynomials and covering systems of congruences, *Acta Aritm.* **13** (1967), 91–101.

Proof Without Words: Sums of Triangular Numbers

$$t_n = 1 + 2 + \cdots + n \Rightarrow t_1 + t_2 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}$$



$$t_1 + t_2 + \cdots + t_n = \frac{1}{6}(n+1)^3 - (n+1)\cdot\frac{1}{6} = \frac{n(n+1)(n+2)}{6}$$

—Roger B. Nelsen
Lewis & Clark College
Portland OR 97219

On the Metamorphosis of Vandermonde's Identity

DON RAWLINGS
LAWRENCE SZE
California Polytechnic State University
San Luis Obispo, CA 93407
drawling@calpoly.edu
lsze@calpoly.edu

As motivation for our designs, first consider the identity

$$\sum_{l=0}^{n}\binom{n}{l}=2^n.$$

Next, imagine inserting $a^{n-l}b^l$ in the lth term of the sum and replacing 2^n by $(a+b)^n$. The result is the binomial theorem.

Our objective here is to examine the effect of an analogous "pollination" of Vandermonde's identity

$$\sum_{l=0}^{i}\binom{j}{l}\binom{n-j}{i-l}=\binom{n}{i}. \tag{1}$$

Guided by our binomial theorem example, we slip four letters (two per binomial coefficient) with exponents that add to n inside the sum in (1) to obtain

$$\sum_{l=0}^{i}\binom{j}{l}\binom{n-j}{i-l}a^{n+l-i-j}b^{j-l}c^{i-l}d^l. \tag{2}$$

Although there is no simple formula for this sum to rival the $(a+b)^n$ of the binomial identity, an interesting metamorphosis ensues, producing a noteworthy matrix identity.

For convenience, we abbreviate the sum in (2) by $V_{i,j}\binom{a,b}{c,d}$. The leading role in our story is played by the matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}_n = \left(V_{i,j}\binom{a,b}{c,d}\right)_{0\le i,j\le n}, \tag{3}$$

which we shall refer to as the nth *Vandermonde matrix* with parameters a, b, c, and d. For $n=3$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}_3 = \begin{pmatrix} a^3 & a^2b & ab^2 & b^3 \\ 3a^2c & 2abc+a^2d & b^2c+2abd & 3b^2d \\ 3ac^2 & bc^2+2acd & 2bcd+ad^2 & 3bd^2 \\ c^3 & c^2d & cd^2 & d^3 \end{pmatrix}. \tag{4}$$

At least two cases of the Vandermonde matrix have already achieved some notoriety. When $c=0$ and $a=b=d=1$, (3) is upper triangular and contains the first $n+1$ rows of Pascal's triangle. For instance,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}_3 = \left(V_{i,j}\binom{1,1}{0,1}\right)_{0\le i,j\le 3} = \left(\binom{j}{i}\right)_{0\le i,j\le 3} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

When transposed, this case of (3) is aptly referred to as the nth Pascal matrix. The case of (3) with $c = 0$ and $a = d = 1$ has also received some attention. It coincides with the transpose of a generalization of Pascal's matrix considered first by Call and Velleman [**2**] and later by Aggarwala and Lamoureux [**1**].

Getting back to our story, our pollination of the sum in (2) leads to the following result.

THEOREM 1. *If $a, b, \ldots, g$ are elements of a field, then*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}_n \begin{bmatrix} e & f \\ g & h \end{bmatrix}_n = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right]_n. \tag{5}$$

In other words, the product of two Vandermonde matrices is Vandermonde. Moreover, the matrix of parameters for the product miraculously coincides with the product of the underlying two-by-two matrices of parameters!

Before proving (5), we present a sampling of its remarkable implications in the next two sections. In the final section, we briefly describe the context that led us to Theorem 1.

A sampler of inverses and determinants The most amusing consequences of Theorem 1 involve inverses and determinants of Vandermonde matrices. For $ad - bc \neq 0$, (5) implies that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}_n^{-1} = \begin{bmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix}_n = \frac{1}{(ad-bc)^n}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}_n. \tag{6}$$

As an example of (6), the inverse of the transpose of Pascal's matrix is readily seen to be

$$\left(\binom{j}{i}\right)_{0\le i,j\le n}^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}_n^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}_n = \left((-1)^{j-i}\binom{j}{i}\right)_{0\le i,j\le n}.$$

So, for $n = 3$,

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -2 & 3 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Although the origin of this equality is unclear to us, it is well known and appears in a number of contexts (including inclusion-exclusion [**5**, p. 67]).

Next, we note that the determinant of the Vandermonde matrix is just a power of the determinant of its underlying two-by-two matrix of parameters.

COROLLARY 1.

$$\det\begin{bmatrix} a & b \\ c & d \end{bmatrix}_n = (ad - bc)^{n(n+1)/2}.$$

Proof. The result follows directly if a, b, c, or d is zero; for instance, if $c = 0$, then (3) (the example in (4) is illustrative) is upper triangular with ith diagonal entry $a^{n-i}d^i$ for $0 \le i \le n$. Thus,

$$\det\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}_n = a^n d^0 a^{n-1} d^1 \cdots a^0 d^n = (ad - b\cdot 0)^{n(n+1)/2}.$$

So assume that a, b, c, and d are all nonzero. As

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}_n = \begin{bmatrix} (ad-bc)/d & b/d \\ 0 & 1 \end{bmatrix}_n \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix}_n \tag{7}$$

and as the determinant of a product is the product of determinants, we have

$$\det\begin{bmatrix} a & b \\ c & d \end{bmatrix}_n = \left(\frac{ad-bc}{d}\right)^{n(n+1)/2} d^{n(n+1)/2} = (ad-bc)^{n(n+1)/2}. \qquad \blacksquare$$

Corollary 1 bears a resemblance to the classical *Vandermonde determinant*

$$\det(x_i^{n-j})_{0\le i,j\le n} = \prod_{0\le i<j\le n} (x_i - x_j).$$

Motivated by the similarities, we tried introducing even more variables, indexing our parameters a and b by row. The result in (8) below, which we refer to as the Vandermonde expansion, may be regarded as a distant cousin of the binomial theorem.

For $\vec{a} = (a_0, a_1, \dots, a_n)$ and $\vec{b} = (b_0, b_1, \dots, b_n)$, let

$$\begin{bmatrix} \vec{a} & \vec{b} \\ c & d \end{bmatrix}_n = \left(V_{i,j}\binom{a_i, b_i}{c, d}\right)_{0\le i,j\le n}.$$

Then, a slight variation on our proof of Corollary 1 leads to

$$\det\begin{bmatrix} \vec{a} & \vec{b} \\ c & d \end{bmatrix}_n = (a_0 d - b_0 c)^n (a_1 d - b_1 c)^{n-1} \cdots (a_n d - b_n c)^0. \tag{8}$$

The key is to observe that the matrix on the extreme right in (7) is independent of a and b. So (7) remains true when, in both of the other matrices, the a and b in row i are respectively replaced by a_i and b_i for $0 \le i \le n$.

Although the Vandermonde expansion will never become as popular as the binomial theorem, it contains some striking special cases. When $n = 3$, $c = -1$, $d = 1$, $\vec{a} = (a, 1, 1, 1)$, and $\vec{b} = (b, 0, 0, 0)$, (8) reduces to

$$(a+b)^3 = \begin{vmatrix} a^3 & a^2b & ab^2 & b^3 \\ -3 & 1 & 0 & 0 \\ 3 & -2 & 1 & 0 \\ -1 & 1 & -1 & 1 \end{vmatrix}.$$

In the above, note that the usual suspects in the expansion of $(a+b)^3$ appear across the first row and that a truncated, signed Pascal triangle is contained in the lower left corner. Of course, such determinant formulas for $(a+b)^k$, $0 \le k \le n(n+1)/2$, may be obtained by simply running monomials through appropriate rows of the signed Pascal triangle. For instance, if $n = 3$, $c = -1$, $d = 1$, $\vec{a} = (a, a, 1, 1)$, and $\vec{b} = (b, b, 0, 0)$, then (8) implies

$$(a+b)^5 = \begin{vmatrix} a^3 & a^2b & ab^2 & b^3 \\ -3a^2 & a^2-2ab & 2ab-b^2 & 3b^2 \\ 3 & -2 & 1 & 0 \\ -1 & 1 & -1 & 1 \end{vmatrix}.$$

Among the outright curious, the balanced selections $\vec{a} = (a, 1/2, 1/2, 1/2)$ and $\vec{b} = (b, 1/2, 1/2, 1/2)$ with $n = 3$, $c = -1$, and $d = 1$ in (8) give

$$(a+b)^3 = \begin{vmatrix} a^3 & a^2b & ab^2 & b^3 \\ -3/4 & -1/4 & 1/4 & 3/4 \\ 3/2 & -1/2 & -1/2 & 3/2 \\ -1 & 1 & -1 & 1 \end{vmatrix}.$$

A sampler of scalar identities Theorem 1 is a cache of binomial identities ranging from the well-known to the exotic. Careful selection of the parameters will in fact reveal Vandermonde's identity, the binomial theorem, and other results of interest. First, by the definition of matrix multiplication, (5) is equivalent to

$$\sum_{k=0}^{n} V_{i,k}\begin{pmatrix} a, b \\ c, d \end{pmatrix} V_{k,j}\begin{pmatrix} e, f \\ g, h \end{pmatrix} = V_{i,j}\begin{pmatrix} ae+bg, af+bh \\ ce+dg, cf+dh \end{pmatrix}, \tag{9}$$

where j is any integer from 0 to n.

To extract (1) from (9), note that

$$V_{i,k}\begin{pmatrix} 1, 0 \\ 1, 0 \end{pmatrix} = \sum_{l=0}^{i} \binom{k}{l}\binom{n-k}{i-l} 1^{n+l-i-k} 0^{k-l} 1^{i-l} 0^{l} = \begin{cases} \binom{n}{i} & \text{if } k=0, \\ 0 & \text{if } 0 < k \le n. \end{cases}$$

Similarly,

$$V_{k,j}\begin{pmatrix} 1, 1 \\ 0, 1 \end{pmatrix} = \sum_{l=0}^{k} \binom{j}{l}\binom{n-j}{k-l} 1^{n+l-k-j} 1^{j-l} 0^{k-l} 1^{l} = \binom{j}{k}.$$

Thus, we obtain (1):

$$\binom{n}{i} = \sum_{k=0}^{n} V_{i,k}\begin{pmatrix} 1, 0 \\ 1, 0 \end{pmatrix} V_{k,j}\begin{pmatrix} 1, 1 \\ 1, 0 \end{pmatrix} = V_{i,j}\begin{pmatrix} 1, 1 \\ 1, 1 \end{pmatrix} = \sum_{l=0}^{i} \binom{j}{l}\binom{n-j}{i-l}.$$

Of course, further setting $j = 1$ gives the well-known binomial recurrence

$$\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}. \tag{10}$$

To see the binomial theorem emerge from (9), observe that

$$V_{0,k}\begin{pmatrix} a, b \\ a, b \end{pmatrix} = a^{n-k}b^{k} \quad \text{and} \quad V_{k,0}\begin{pmatrix} 1, 1 \\ 1, 1 \end{pmatrix} = \binom{n}{k}.$$

So

$$(a+b)^n = V_{0,0}\begin{pmatrix} a+b, a+b \\ a+b, a+b \end{pmatrix} = \sum_{k=0}^{n} V_{0,k}\begin{pmatrix} a, b \\ a, b \end{pmatrix} V_{k,0}\begin{pmatrix} 1, 1 \\ 1, 1 \end{pmatrix} = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k}.$$

In the realm of the exotic, we note that the special case

$$\sum_{k=0}^{n} V_{i,k}\begin{pmatrix} 1, -1 \\ 1, \ \ 1 \end{pmatrix} V_{k,j}\begin{pmatrix} 1, 1 \\ 2, 1 \end{pmatrix} = V_{i,j}\begin{pmatrix} -1, 0 \\ 3, 2 \end{pmatrix}$$

of (9) translates into

$$\sum_{k=0}^{n}\sum_{m=0}^{i}\sum_{l=0}^{k} (-1)^{k-m}\binom{k}{m}\binom{n-k}{i-m}\binom{j}{l}\binom{n-j}{k-l} 2^{k-l} = (-1)^{n-i}\binom{n-j}{i-j} 2^{j} 3^{i-j}.$$

Closed formulas for such sums are easily produced. The trick is to select $a, b, \ldots, h$ so that at least one of the parameters on the right in (9) is zero.

Next, as Vandermonde's identity (1) holds when j is viewed as an indeterminate, it is only natural to ask whether (9) has a similar extension. Annoyingly, the answer in general is no. Recall that for j an indeterminate and l a nonnegative integer, the extended binomial coefficient is defined by

$$\binom{j}{l} = \begin{cases} \dfrac{j(j-1)\cdots(j-l+1)}{l!} & \text{if } l > 0, \\ 1 & \text{if } l = 0. \end{cases} \tag{11}$$

Of course, (11) agrees with the usual binomial coefficient when j is replaced by an integer greater than or equal to l. Also, (11) is a polynomial in j of degree l. The difficulty in extending (9) is exposed by noting that, if j is a real number other than $0, 1, \ldots,$ or n, then

$$\sum_{k=0}^{n} V_{i,k}\binom{0,1}{0,1} V_{k,j}\binom{0,0}{0,1} = \binom{n}{i}\binom{j}{n} \neq 0^{n-j}\binom{n}{i} = V_{i,j}\binom{0,1}{0,1}.$$

However, (9) may be extended with some restrictions.

One approach, among many, is to restrict $a, b, \ldots, h$ to the field of real numbers and require that

$$eh = gf \qquad \text{and that } e, f, ae+bg \text{ and } af+bh \text{ are all positive.} \tag{12}$$

The proof that (9) holds under these conditions parallels the standard technique for extending (1): First, for $0 \leq k \leq n$, note that

$$e^j f^{-j} V_{k,j}\binom{e,f}{g,h} = \sum_{l=0}^{k}\binom{j}{l}\binom{n-j}{k-l} e^{n+l-k} f^{-l} g^{k-l} h^l$$

is a polynomial in j of degree at most k. Now, for $0 \leq i \leq n$, define

$$p(j) = e^j f^{-j} V_{i,j}\binom{ae+bg,\, af+bh}{ce+dg,\, cf+dh} - e^j f^{-j}\sum_{k=0}^{n} V_{i,k}\binom{a,b}{c,d} V_{k,j}\binom{e,f}{g,h}.$$

With (12) in mind and a little work, it may be verified that $p(j)$ is a polynomial in j of degree at most n. As (9) implies that $p(j)$ has at least $n+1$ roots (namely, $0, 1, \ldots, n$), $p(j)$ must in fact be the zero polynomial. Thus, under the terms of (12), (9) holds for j an indeterminate.

As a final example, we note that setting $a = c = e = f = 1, b = d = g = h = 0$, and $j = -1$ in our extension of (9) gives the commonplace equality

$$\binom{n}{i} = \sum_{l=0}^{i}(-1)^l\binom{n+1}{i-l}.$$

An algebraic proof There are a number of proofs of Theorem 1. For one, it is possible to extend the usual combinatorial proof of (1). It is not too difficult to see that the sum in (2) may be interpreted as a *weighted* selection of a committee of size i from a group of people consisting of j women and $n-j$ men. Induction will also do the job: With judicious use of (10), it may be verified that both sides of (9) (which, we recall, is equivalent to (5) in Theorem 1) satisfy the recurrence relationship

$$\rho_{i,j}(n) = (af+bh)\rho_{i,j-1}(n-1) + (cf+dh)\rho_{i-1,j-1}(n-1).$$

However, we find neither the combinatorial approach nor the induction argument entirely satisfying. In our opinion, the slickest proof, the only one we present, relies on linear algebra.

We set the stage. Let V be an m-dimensional vector space with ordered basis $\beta = (\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_m)$. The matrix representation relative to β of a linear operator $T : V \to V$ is $[T]_\beta = (a_{i,j})_{1\le i,j\le m}$, where $a_{i,j}$ is the ith coordinate of $T(\vec{v}_j)$, that is, the $a_{i,j}$ are scalars satisfying

$$T(\vec{v}_j) = \sum_{i=1}^{m} a_{i,j}\vec{v}_i \quad \text{for} \quad 1 \le j \le m.$$

The algebraic key to (5) is the fact that the matrix associated with the composition of linear operators is the product of the matrices of the operators. In other words, if $S, T : V \to V$ are linear operators, then (see Friedberg, Insel, and Spence [**3**, Ch. 2])

$$[S \circ T]_\beta = [S]_\beta [T]_\beta. \tag{13}$$

Identity (13) is a handy tool for establishing properties of matrix multiplication that avoids much of the tedium of indices! It's perfect for our purposes.

Proof of Theorem 1. Let F denote a field, $a, b, \ldots, h$ be elements of F, and $F[x, y]$ be the ring of polynomials over F in the commuting indeterminates x and y. For each polynomial $p(x, y) \in F[x, y]$, define

$$M(p) = p(ax + cy, bx + dy) \quad \text{and} \quad N(p) = p(ex + gy, fx + hy).$$

By thinking in terms of matrix products, we may express the formulas for M and N in the more satisfying forms

$$M(p) = p\left((x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \quad \text{and} \quad N(p) = p\left((x, y)\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right). \tag{14}$$

Note that $M, N : F[x, y] \to F[x, y]$. Also, both M and N are ring homomorphisms. From (14), the composition of M with N applied to a polynomial $p(x, y) \in F[x, y]$ is seen to be

$$M \circ N(p) = p\left((x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right).$$

We now turn our attention to the subset

$$H_n = \{a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n : a_0, a_1, \ldots, a_n \in F\}$$

of $F[x, y]$. The nonzero elements in H_n are just the homogeneous polynomials of degree n in the indeterminates x and y. Note that H_n is a vector space over F and that $\gamma = (x^n, x^{n-1}y, \ldots, y^n)$ constitutes an ordered basis of H_n. Moreover, the restrictions of M and N to H_n are linear operators on H_n.

To determine the matrix of M relative to the ordered basis γ, we fish the coefficient of $x^{n-i}y^i$ out of

$$M(x^{n-j}y^j) = (ax + cy)^{n-j}(bx + dy)^j. \tag{15}$$

For $0 \le l \le i$, the binomial theorem tells us that the coefficient of

$$x^{n+l-i-j}y^{i-l} \quad \text{in} \quad (ax + cy)^{n-j} \quad \text{is} \quad \binom{n-j}{i-l}a^{n+l-i-j}c^{i-l}$$

and that the coefficient of

$$x^{j-l}y^l \quad \text{in} \quad (bx+dy)^j \quad \text{is} \quad \binom{j}{l} b^{j-l}d^l.$$

Noting that $x^{n-i}y^i = x^{n+l-i-j}y^{i-l}x^{j-l}y^l$ for $0 \le l \le i$, it is then evident that the coefficient of $x^{n-i}y^i$ in (15) is none other than

$$\sum_{l=0}^{i} \binom{j}{l}\binom{n-j}{i-l} a^{n+l-i-j}b^{j-l}c^{i-l}d^l = V_{i,j}\binom{a,b}{c,d}.$$

So the matrix relative to γ of M restricted to H_n is

$$[M]_\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}_n.$$

As similar considerations lead to

$$[N]_\gamma = \begin{bmatrix} e & f \\ g & h \end{bmatrix}_n \quad \text{and} \quad [M \circ N]_\gamma = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right]_n,$$

(13) delivers the final blow:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}_n \begin{bmatrix} e & f \\ g & h \end{bmatrix}_n = [M]_\gamma[N]_\gamma = [M \circ N]_\gamma = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right]_n. \quad \blacksquare$$

For the adventurous, we note that our algebraic proof is readily adapted to deduce identities for *extended* Vandermonde matrices with k^2 parameters for any integer $k \ge 2$.

Concluding remarks We were led to consider the pollinated sum (2) and to the discovery of Theorem 1 by certain practical considerations. There are many natural contexts in which the elements of a fixed set vary with time between two states. For one, the members of a given population may or may not have a certain contagious disease. From one moment to the next, a healthy individual may become ill and an infected individual may recover. For another, the components of a system of service may either be in or out of service. Again, with each passing moment, an in-service component may fail while a broken component may be repaired and returned to service. It turns out that, under certain probabilistic assumptions, such processes can be modeled as Markov chains. Moreover, the corresponding transition matrices are Vandermonde.

In this context, Theorem 1 is an indispensable tool. It allows us to manipulate (multiply, invert, and diagonalize) Vandermonde matrices at will. As we've demonstrated, such computations miraculously boil down to working with the underlying two-by-two matrices of associated parameters.

REFERENCES

1. R. Aggarwala and M. P. Lamoureux, Inverting the Pascal matrix plus one, *Amer. Math. Monthly* **109** (2002), 371–377.
2. G. S. Call and D. J. Velleman, Pascal's matrices, *Amer. Math. Monthly* **100** (1993), 372–376.
3. S. Friedberg, A. Insel, and L. Spence, *Linear Algebra*, third edition, Prentice Hall, NJ, 1997.
4. D. Rawlings and L. Sze, On the reliability of an n-component system, in preparation.
5. R. P. Stanley, *Enumerative Combinatorics* Vol. I, Wadsworth and Brooks/Cole, Pacific Grove, CA, 1986.

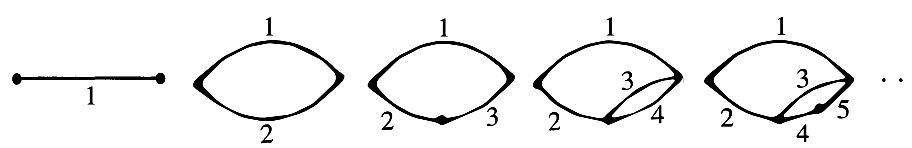
PROBLEMS

Proposals

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

1721. *Proposed by Donald Knuth, Stanford University, Stanford, CA.*

The *Fibonacci graphs*



are defined by successively replacing the edge with maximum label n by two edges n and $n+1$, in series if n is even, and in parallel if n is odd. Prove that the Fibonacci graph with n edges has exactly F_{n+1} spanning trees, where $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$. Show also that these spanning trees can be listed in such a way that some edge k is replaced by $k \pm 1$ as we pass from one tree to the next. For example, for $n = 5$ the eight spanning trees can be listed as 125, 124, 134, 135, 145, 245, 235, 234.

1722. *Proposed by Emeric Deutsch, Polytechnic University, Broooklyn, NY.*

Let k and n be positive integers with $k \leq n$. Find the number of permutations of $\{1, 2, \ldots, n\}$ in which $1, 2, \ldots, k$ appears as a subsequence but $1, 2, \ldots, k, k+1$ does not.

1723. *Proposed by Herb Bailey, Rose Hulman Institute of Technology, Terre Haute, IN.*

Let I be the incenter of triangle ABC with BC tangent to the incircle at D. Let E be the intersection of the extension of $\overline{ID}$ with the circle through B, I, and C. Prove that

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.

$$\overline{DE} = \frac{T}{s-a},$$

were T and s are, respectively, the area and semiperimeter of triangle ABC, and $a = \overline{BC}$.

1724. *Proposed by Mihály Bencze, Săcele-Négyfalu, Romania.*

Let $x_1, x_2, \ldots, x_n$ be positive real numbers. Prove that

$$\frac{1}{n}\sum_{k=1}^{k} x_k - \left(\prod_{k=1}^{n} x_k\right)^{1/n} \leq \frac{1}{n}\sum_{1\leq j<k\leq n} (\sqrt{x_j} - \sqrt{x_k})^2.$$

1725. *Proposed by Michel Bataille, Rouen, France.*

Let $\mathcal{E}$ be the ellipse with equation $x^2/a^2 + y^2/b^2 = 1$, where a and b are positive integers. Find the number of parallelograms with vertices at integer lattice points and sides tangent to $\mathcal{E}$ at their midpoints.

Quickies

Answers to the Quickies are on page 243.

Q951. *Proposed by Ovidiu Furdui, student, Western Michigan University, Kalamazoo, MI.*

Show that

$$\int_0^\infty \int_0^\infty \frac{\sin^2 x \sin^2 y}{x^2(x^2+y^2)}\, dx\, dy = \frac{\pi^2}{8}.$$

Q952. *Proposed by Erwin Just (Emeritus) and Norman Schaumberger (Emeritus), Bronx Community College of the City University of New York, New York, NY.*

Let n be a positive integer and let $x_1, x_2, \ldots, x_n$ be positive real numbers with $x_1 x_2 \cdots x_n \geq 1$. Prove that for any positive integer k,

$$\sum_{j=1}^{n} x_j^k \geq \sum_{j=1}^{n} x_j^{k-1},$$

with equality if and only if $x_1 = x_2 = \cdots = x_n = 1$.

Solutions

A Diophantine Equation **June 2004**

1696. *Proposed by Albert F. S. Wong, Singapore.*

For which positive integers k does the equation

$$x^{2k-1} + y^{2k} = z^{2k+1}$$

have a solution in positive integers x, y, and z?

Solution by Jerry W. Grossman, Oakland University, Rochester, MI.

There are solutions for all k. Because $2k-1$, $2k$, and $2k+1$ are pairwise relatively prime, it follows from the Chinese Remainder Theorem that there is a positive integer m with

$$m \equiv 0 \pmod{2k}$$
$$m \equiv 0 \pmod{2k+1}$$
$$m \equiv -1 \pmod{2k-1}.$$

There are then positive integers r, s, t with $m = r(2k) = s(2k+1) = t(2k-1) - 1$. Now let $a = 3^{2k+1} - 2^{2k}$, so $a + 2^{2k} = 3^{2k+1}$. Multiply through by a^m to obtain $a^{m+1} + a^m 2^{2k} = a^m 3^{2k+1}$. This can be put into the form

$$(a^t)^{2k-1} + (2a^r)^{2k} = (3a^s)^{2k+1},$$

giving a solution to the diophantine equation.

Note. Daniele Donini notes that in the article "On Solutions of the Equation $x^a + y^b = z^c$", in the MAGAZINE **41**:4 (1968), 174–5, Allan I. Liff shows that the equation $x^a + y^b = z^c$ is solvable in positive integers if at least one of the exponents is relatively prime to the other two.

Also solved by JPV Abad, Reza Akhlaghi, Roy Barbara (Lebanon), Michel Bataille (France), Eddie Cheng, John Christopher, Con Amore Problem Group (Denmark), Jim Delany, Boian Djonov, Daniele Donini (Italy), Anne-Maria Ernvall-Hytönen (Finland), G.R.A.20 Problems Group (Italy), Chris Hill, David P. Lang, Peter W. Lindstrom, David E. Manes, José H. Nieto (Venezuela), Walter Nissen, Northwestern University Math Problem Solving Group, Thomas Peter, Iwan Praton, Achilleas Sinefakopoulos, Ian VanderBurgh, Paul Weisenhorn (Germany), Steven J. Wilson, Li Zhou, and the proposer.

Connected Permutations **June 2004**

1697. *Proposed by David Callan, University of Wisconsin, Madison, WI.*

A permutation π on $[n] = \{1, 2, \ldots, n\}$ is *connected* if for each k, $1 \le k \le n-1$, there is a j, $1 \le j \le k$ with $\pi(j) > k$. Let a_n denote the number of connected permutations on $[n]$. Show that for $n \ge 2$,

$$a_n = \sum_{k=1}^{n-1} k(n-k-1)!\, a_k.$$

Solution by Jim Delany, California Polytechnic State University, San Luis Obispo, CA.

For positive integer k, let $[k] = \{1, 2, \ldots, k\}$. Let π be a permutation on $[n]$. We say π is k-disjoint if $\pi([k]) = [k]$, but $\pi([j]) \neq [j]$ for $j < k$. Let D_k be the set of k-disjoint permutations on $[n]$. The sets D_k partition the set of permutations on $[n]$, and a permutation π is connected if and only if $\pi \in D_n$. If $\pi \in D_k$, then restricting π to $[k]$ results in a connected permutation on $[k]$. It follows that $|D_k| = (n-k)!\, a_k$, and hence that $n! = \sum_{k=1}^{n}(n-k)!\, a_k$. Applying this to the sum in question,

$$\begin{aligned}\sum_{k=1}^{n-1} k(n-k-1)!\, a_k &= \sum_{k=1}^{n-1} (n-(n-k))\,(n-k-1)!\, a_k \\ &= \sum_{k=1}^{n-1} n(n-k-1)!\, a_k - \sum_{k=1}^{n-1}(n-k)!\, a_k\end{aligned}$$

$$= n\sum_{k=1}^{n-1}((n-1)-k)!\,a_k - \left(\sum_{k=1}^{n}(n-k)!\,a_k - a_n\right)$$
$$= n(n-1)! - (n! - a_n) = a_n.$$

Note. Chip Curtis notes that connected permutations are called *indecomposable* by R. P. Stanley in *Enumerative Combinatorics, Volume I*, Cambridge University Press, 1999, p. 49. The first few terms of the sequence $\{a_n\}$ are $1, 1, 3, 13, 71, 461, \ldots$. At the website http://www.research.att.com/~njas/sequences, this is sequence A003319. This site also provides the following explicit formula,

$$a_n = (-1)^{n-1}\det\begin{pmatrix} 1! & 2! & 3! & \ldots & n! \\ 1 & 1! & 2! & \ldots & (n-1)! \\ 0 & 1 & 1! & \ldots & (n-2)! \\ & & & \vdots & \\ 0 & 0 & 0 & \ldots & 1! \end{pmatrix}.$$

Also solved by JPV Abad, Michel Bataille (France), Con Amore Problem Group (Denmark), Chip Curtis, Jim Delany, Daniele Donini (Italy), Elias Lampakis (Greece), José H. Nieto (Venezuela), Rob Pratt, Nicholas C. Singer, Christopher N. Swanson, Li Zhou, and the proposer.

A Rational Expression **June 2004**

1698. *Proposed by Achilleas Sinefakopoulos, student, Cornell University, Ithaca, NY.*

Let n be an odd positive integer and let r be a positive rational number. Prove that there are positive integers $a_1, a_2, a_3, b_1, b_2, b_3$ such that

$$r = \frac{a_1^n + a_2^{n+1} + a_3^{n+2}}{b_1^n + b_2^{n+1} + b_3^{n+2}}.$$

Solution by Chris Hill, St. Bonaventure University, St. Bonaventure, NY.

Let $r = p/q$, where p and q are positive integers. Then

$$\frac{\left(p^{(n+1)/2}q^{(n+3)/2}\right)^n + \left(pq^{n-1}\right)^{n+1} + (pq^n)^{n+2}}{(pq^n)^n + \left(pq^{n+1}\right)^{n+1} + \left(p^{(n-1)/2}q^{(n+1)/2}\right)^{n+2}}$$
$$\frac{p}{q}\cdot\frac{p^{(n^2+n)/2-1}q^{(n^2+3n)/2} + p^nq^{n^2-1} + p^{n+1}q^{n^2+2n}}{p^nq^{n^2-1} + p^{n+1}q^{n^2+2n} + p^{(n^2+n)/2-1}q^{(n^2+3n)/2}} = \frac{p}{q}.$$

Thus p/q has the desired representation and we may choose $b_1 = a_3$.

Also solved by John Christopher, Con Amore Problem Group (Denmark), Daniele Donini (Italy), Li Zhou, and the proposer.

A Tetrahedron Inequality **June 2004**

1699. *Proposed by Zhang Yun, First Middle School of Jinchung City, Gan Su, China.*

Let $A_1A_2A_3A_4$ be a nondegenerate tetrahedron, let h_k, $1 \le k \le 4$, be the length of the altitude from A_k, and let r be the radius of the inscribed sphere. Prove that

$$\frac{h_1}{h_1+3r} + \frac{h_2}{h_2+3r} + \frac{h_3}{h_3+3r} + \frac{h_4}{h_4+3r} \ge \frac{16}{7}.$$

Solution by Michel Bataille, Rouen, France.

Let S_k be the area of the face opposite A_k, $1 \le k \le 4$, and $S = S_1 + S_2 + S_3 + S_4$. The volume V of $A_1A_2A_3A_4$ is given by $V = \frac{1}{3}h_kS_k$, $1 \le k \le 4$, and by $V = \frac{1}{3}rS$. Thus, $r/h_k = S_k/S$, $1 \le k \le 4$. We then have

$$\sum_{k=1}^{4} \frac{h_k}{h_k + 3r} = \sum_{k=1}^{4} \frac{1}{1 + 3(r/h_k)} = \sum_{k=1}^{4} \frac{1}{1 + 3(S_k/S)} \ge \frac{4}{\frac{1}{4}\sum_{k=1}^{4}(1 + 3(S_k/S))} = \frac{16}{7},$$

where the inequality follows from the arithmetic-harmonic mean inequality. Furthermore, equality holds if and only if $S_1 = S_2 = S_3 = S_4$, that is, if and only if $A_1A_2A_3A_4$ is an isosceles tetrahedron.

Also solved by Minh Can, Chip Curtis, Daniele Donini (Italy), Michael Goldenberg and Mark Kaplan, G.R.A.20 Problems Group (Italy), D. Kipp Johnson, L. R. King, Murray S. Klamkin (Canada), Kee-Wai Lau (China), José H. Nieto (Venezuela), Northwestern University Math Problem Solving Group, Raul A. Simon (Chile), Ian VanderBurgh (Canada), Li Zhou, and the proposer.

A Condition for $AB = BA$ June 2004

1700. *Proposed by Yongge Tian, Queen's University, Kingston, Ontario, Canada.*

Let A and B be $n \times n$ matrices satisfying $A^2 = A$ and $B^2 = B$. Show that $AB = BA$ if and only if range(AB) = range(BA) and range(A^TB^T) = range(B^TA^T), where C^T denotes the transpose of C.

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

Suppose that range(AB) = range(BA) and range(A^TB^T) = range(B^TA^T). Then by **[1]**, there are invertible $n \times n$ matrices P and Q such that

$$AB = BAP \quad \text{and} \quad A^TB^T = B^TA^TQ.$$

Multiplying (1) on the left by B we get $BAB = B^2AP = BAP = AB$. Transposing (2) into $BA = Q^TAB$ and multiplying on the right by B we get $BAB = Q^TAB^2 = Q^TAB = BA$. Hence $AB = BA$. The converse is immediate.

REFERENCE

1. C. D. Meyer, *Matrix Analysis and Linear Algebra*, SIAM, 2000, p. 171.

Also solved by Michael Andreoli, Michel Bataille (France), Gary F. Birkenmeier, Chico Problem Students, Adam Coffman, Luz M. DeAlba, Jim Delany, Daniele Donini (Italy), Eugene A. Herman, Mandy Hill and Lucian Stanisor and Aminiel Awichi and Amy Ward, David P. Lang, Junaid N. Mansuri, José H. Nieto (Venezuela), Patricia Parker and Brandi Shuptrine and Tiffany Jackson and Chuck Miller, Daniel R. Patten, Angela Sanders and Kelly Nichole Troillet, Gerald Thompson, Thai-Doung Tran, Götz Trenkler (Germany), University of Arkansas Little Rock Solvers, Xiaoshen Wang, Yan-loi Wong (Singapore), and the proposer.

Answers

Solutions to the Quickies from page 240.

A951. Let I denote the value of the integral. Then

$$I = \int_0^\infty \frac{\sin^2 x}{x^2}\left(\int_0^\infty \frac{\sin^2 y}{x^2 + y^2}\,dy\right)dx = \int_0^\infty \frac{\sin^2 y}{y^2}\left(\int_0^\infty \frac{\sin^2 x}{x^2 + y^2}\,dx\right)dy$$
$$= \int_0^\infty \int_0^\infty \frac{\sin^2 x \sin^2 y}{y^2(x^2 + y^2)}\,dx\,dy.$$

Thus

$$2I = \int_0^\infty \int_0^\infty \left(\frac{\sin^2 x \sin^2 y}{x^2(x^2+y^2)} + \frac{\sin^2 x \sin^2 y}{y^2(x^2+y^2)} \right) dx\, dy$$
$$= \int_0^\infty \int_0^\infty \frac{\sin^2 x \sin^2 y}{x^2 y^2}\, dx\, dy = \left(\int_0^\infty \frac{\sin^2 x}{x^2}\, dx \right) \left(\int_0^\infty \frac{\sin^2 y}{y^2}\, dy \right) = \frac{\pi^2}{4}.$$

The result follows.

A952. If $k \geq 2$ we have

$$\sum_{j=1}^n x_j^k - \sum_{j=1}^n x_j^{k-1} = \sum_{j=1}^n (x_j^k - x_j^{k-1})$$
$$= \sum_{j=1}^n \left((x_j - 1)(x_j^{k-1} - 1) + (x_j - 1) \right)$$
$$= \sum_{j=1}^n \left[(x_j - 1) \left((x_j - 1)(x_j^{k-2} + x_j^{k-3} + \cdots + 1) \right) + (x_j - 1) \right]$$
$$= \sum_{j=1}^n (x_j - 1)^2 (x_j^{k-2} + x_j^{k-3} + \cdots + 1) + \left(\sum_{j=1}^n x_j - n \right).$$

The first sum in the last line of the display is clearly nonnegative. The second expression in this line is also nonnegative because

$$\sum_{j=1}^n x_j \geq n \left(\prod_{j=1}^n x_j \right)^{1/n} \geq n.$$

(Note that this also establishes the inequality in the case $k = 1$.) In addition, the last line of the display is 0 if and only if $x_1 = x_2 = \cdots = x_n = 1$.

"Descartes" of Your Dreams

Mathematicians in the market for a car today have many choices. While analytic geometers might be drawn to the ***Ford Focus*** and algebraists may assume the ***Isuzu Axiom*** is for them, graph theorists would probably still choose a ***Nissan Pathfinder***. For linear drivers, there's the ***Toyota Matrix***, but if its dimensions are too large, the ***Honda Element*** is an option. Though the ***Oldsmobile Delta 88*** attracted analysts in the past, ***Infiniti*** currently offers them boundless choices.

Alas, my heart is set on a concept car, the ***Lincoln Lemma***, but I'm waiting for them to work out the details.

——DAWN W. LINDQUIST
UNIVERSITY OF ST. FRANCIS
JOLIET, IL 60435

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.

Seely, Ron, Consumed by a problem: UW–Madison grad student makes math history, *Wisconsin State Journal* (18 March 2005) A1, A10. Mackenzie, Dana, "Cranky" proof reveals hidden regularities, *Science* 308 (1 April 2005) 36–37. McKee, Maggie, Classic maths puzzle cracked at last, `NewScientist.com` news service (21 March 2005), `http://www.newscientist.com/article.ns?id=dn7180` .

The numbers of partitions of every positive integer of the form $5n + 4$ are all divisible by 5; for integers of the form $7n + 5$, by 7; for $11n + 6$, by 11. Ramanujan noticed these congruences in 1920, with their mysterious multiplicative structure in an additive problem. The first two were proved by Freeman Dyson in the 1940s, and a general method (a "crank to turn") for all three was found by George Andrews and Frank Garvan. In the late 1990s, Ken Ono (University of Wisconsin) used modular forms to prove that there are such congruences for all larger primes, too. Now Karl Mahlburg, a graduate student of Ono's, has found that "the crank" itself indeed works for all primes. Mahlburg makes press reports and earlier work available at his site `http://www.math.wisc.edu/~mahlburg/`, but not the paper in question. (Thanks to Don Schneider, Beloit, WI.)

The Abel Prize 2005. Press Releases and Biographies. `http://www.abelprisen.no/en/prisvinnere/2005/documents/abelprize_2005_EN.pdf` . Helge Holden, Peter D. Lax: Elements from his contributions to mathematics, `http://www.abelprisen.no/en/prisvinnere/2005/documents/popular2005eng9.pdf` .

Peter D. Lax (Courant Institute, New York University) has been awarded the Abel Prize for 2005 ($986K), for his work in theory and applications of differential equations and computation of their solutions; applications include shock waves and solitons. The explanation of Lax's work by Holden starts out bravely in a popular vein; the second section is entitled, "What is a differential equation?" But it is a tall leap from there to Lax's work: Half a page later we have the heat equation, with its second partial derivatives; and differential operators show up in the last section. The Abel Prize is awarded by the Norwegian Academy of Science and Letters and presented by the King of Norway. The first prize, in 2003, went to Jean-Pierre Serre; the 2004 prize was shared by Michael Atiyah and Isadore Singer. Press reports term the prize "a kind of surrogate for a Nobel prize in mathematics," but it is just as real, just as valuable, and good publicity for mathematics.

Clauset, Aaron, and Maxwell Young, Scale invariance in global terrorism, `http://arxiv.org/abs/physics/0502014` (2 February 2005).

Mathematics is the science of patterns, some of which may surprise us. The authors graph, on a log-log scale, frequency vs. severity of terrorist attacks over the past 37 years. For both injuries and of deaths, they find a power law $x^{-\alpha}$, with $\alpha \approx 1.9$. It resembles that observed by Lewis F. Richardson about wars (with a same-size α). The authors consequently suggest that large-scale events such as the attack on New York City are not "special cases" but fit the pattern, which with $\alpha < 2$ would predict more frequent and more severe attacks.

Odifreddi, Pergiorgio, *The Mathematical Century: The 30 Greatest Problems of the Last 100 Years*, Princeton University Press, 2005; xvi + 204 pp, $27.95. ISBN 0–691–09294–X. Laird, Cameron, Review, *Unix Review* (February 2005), `http://www.unixreview.com/documents/s=9568/ur0502f/ur0502f.htm`.

This is an astonishingly readable, succinct, and wonderful account of twentieth-century mathematics! It is a great book for mathematics majors, students in liberal-arts courses in mathematics, and the general public. I am amazed at how easily the author has set out the achievements in a broad array of mathematical fields. The writing appears effortless. Perhaps a dozen equations appear in all. Laird's review of the book criticizes the chapter on mathematics and the computer—no "wavelets, symbolic algebra, database theory, aleatory methods, or information-based complexity theory, and only a hint of proteomics and cellular automata." Well, it's about mathematics, not computing. (Some concepts mentioned are explained only later or not at all. I hope that the next printing—plus a mass-market paperback at a popular price—fixes a few translation and spelling errors; it wouldn't hurt to re-edit the index, too.)

Preston, Richard, Capturing the unicorn: How two mathematicians came to the aid of the Met, *New Yorker* (11 April 2005) 28–33; `http://www.newyorker.com/fact/content/articles/050411fa_fact`.

Gregory and David Chudnovsky are famous for research in number theory (algorithms for calculating pi) and for building supercomputers (from mail-order parts). Their latest venture turned their supercomputer to fitting together very detailed photographs of parts of the famous "Hunt of the Unicorn" tapestries in the Cloisters museum in Manhattan. They had to match individual threads from one photo to the next, despite shrinking, expanding, and stretching of the fibers over the days of photographing a 15 m^2 tapestry. "Each pixel had to be calculated in its relationship to every other nearby pixel." Three months of computations concluded with a final 24 hours of assembly of the final image. And that was for just one of the seven tapestries.

Conquest, Wendy, Bob Drake, and Dan Rockmore, *The Math Life*, film on NTSC VHS videotape and DVD, Films for the Humanities and Sciences, Princeton, NJ, `www.films.com`, 2002; 51 min, $149.95 (U.S. and Canada distribution only). ISBN 0–7365–5978–7.

This film grapples with what mathematicians do, by interviewing more than a dozen, including Ron Graham, Persi Diaconis, and others famous and not so famous. They say many things that you could anticipate ("we're in the business of abstraction;" "there's this secret world that you can't see unless you know mathematics") and offer an occasional surprising explanation ("[as for] eccentricity levels, mathematics is right at the top because in mathematics you are free to create your own worlds"). Such a film is a rare endeavor, and I enjoyed it. But what does it convey to the nonmathematician audience? As a mathematician, I can't get the beam out of my own eye; but the superficial impressions that come to mind are that about half of mathematicians are foreign-born and that the accompanying technomusic is distracting. As a potential purchaser of such a film (e.g., to show in liberal arts courses on mathematics), I can consider the $150 price either low (compared to an outside speaker) or far too high (compared to PBS films, at $10–20/hour). This film was produced with NSF support; as part of the dissemination plan for the grant, NSF should have demanded a price that a high school teacher could afford.

Mackenzie, Dana, What in the name of Euclid is going on here?, *Science* 307 (4 March 2005) 1402–1403.

Computer software "proof assistants," which check every step of a proof, have been used by Jeremy Avigad (Carnegie Mellon University) to verify the prime number theorem, by Georges Gonthier (Microsoft Research) to verify the proof of the four color theorem, and by Thomas Hales (University of Michigan) to verify the Jordan curve theorem. Hales hopes further to verify his proof of the Kepler conjecture (about optimal sphere-packing).

NEWS AND LETTERS

45th International Mathematical Olympiad

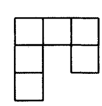
Athens, Greece

July 12 and 13, 2004

edited by Zuming Feng

Problems

1. Let ABC be an acute triangle with $AB \neq AC$, and let O be the midpoint of segment BC. The circle with diameter BC intersects the sides AB and AC at M and N, respectively. The bisectors of $\angle BAC$ and $\angle MON$ meet at R. Prove that the circumcircles of triangles BMR and CNR have a common point lying on segment BC.
2. Find all polynomials $P(x)$ with real coefficients that satisfy the equality
$$P(a-b)+P(b-c)+P(c-a)=2P(a+b+c)$$
for all triples (a, b, c) of real numbers such that $ab+bc+ca=0$.
3. Define a *hook* to be a figure made up of six unit squares as shown in the diagram



or any of the figures obtained by applying rotations and reflections to this figure. Determine all $m \times n$ rectangles that can be tiled with hooks so that

   - the rectangle must be covered without gaps and without overlaps; and
   - no part of a hook may cover area outside the rectangle.

4. Let n be an integer greater than or equal to 3, and let $t_1, t_2, \ldots, t_n$ be positive real numbers such that
$$n^2+1>(t_1+t_2+\cdots+t_n)\left(\frac{1}{t_1}+\frac{1}{t_2}+\cdots+\frac{1}{t_n}\right).$$
Show that t_i, t_j, and t_k are side lengths of a triangle for all i, j, and k with $1 \leq i < j < k \leq n$.
5. In a convex quadrilateral $ABCD$, diagonal BD bisects neither $\angle ABC$ nor $\angle CDA$. Point P lies inside quadrilateral $ABCD$ in such a way that
$$\angle PBC = \angle DBA \quad \text{and} \quad \angle PDC = \angle BDA.$$
Prove that quadrilateral $ABCD$ is cyclic if and only if $AP = CP$.
6. A positive integer is called *alternating* if among any two consecutive digits in its decimal representation, one is even and the other is odd. Find all positive integers n such that n has a multiple that is alternating.

Solutions

Note: For interested readers, the editor recommends the *USA and International Mathematical Olympiads 2004*. There many of the problems are presented together with a collection of remarkable solutions developed by the examination committees, contestants, and experts, during or after the contests.

1. Extend segment AR through R to meet side BC at D (that is, line AD bisects $\angle BAC$). We will prove that the circumcircles of triangles BMR and CNR meet at D. Since quadrilateral $BCNM$ is cyclic,

$$\angle AMN = \angle ACB \quad \text{and} \quad \angle ANM = \angle ABC. \tag{$*$}$$

Hence triangles ABC and ANM are similar. Since $AB \neq AC$, $AN \neq AM$. Because OMN is an isosceles triangle with $OM = ON$, the bisector of $\angle MON$ is also the perpendicular bisector of MN. Because $AM \neq AN$, the intersection of the perpendicular bisector of segment MN and the bisector of $\angle MAN$ meet at a point R on the circumcircle of triangle AMN. We conclude that R lies on the circumcircle of triangle AMN; that is, $AMRN$ is cyclic. It follows that $\angle ARM = \angle ANM$. By the second equality in $(*)$, we obtain $\angle ARM = \angle ABC$. Extend segment AR through to meet side BC at D. Then $\angle ARM = \angle ABD$; that is, $BDRM$ is cyclic. Likewise, we can show that $CDRN$ is cyclic. Therefore, the circumcircles of triangles BMR and CNR meet at D, as desired.

2. A polynomial $P(x)$ satisfies the condition of the problem if and only if $P(x) = c_1x^2 + c_2x^4$, where c_1 and c_2 are arbitrary real numbers.

To see this, assume that $P(x)$ is a polynomial satisfying the conditions of the problem. Set

$$P(x) = p_nx^n + p_{n-1}x^{n-1} + \cdots + p_1x + p_0 = \sum_{i=0}^{n} p_ix^i$$

for real numbers $p_0, p_1, \ldots, p_n$ with $p_n \neq 0$. For a good triple (at, bt, ct), we must have

$$\sum_{i=0}^{n} p_it^i(a-b)^i + \sum_{i=0}^{n} p_it^i(b-c)^i + \sum_{i=0}^{n} p_it^i(c-a)^i = 2\sum_{i=0}^{n} p_it^i(a+b+c)^i,$$

or

$$\sum_{i=0}^{n} p_it^i\left[(a-b)^i + (b-c)^i + (c-a)^i - 2(a+b+c)^i\right] = 0. \tag{$*$}$$

Consider the polynomial $Q(x) = \sum_{i=0}^{n} q_ix^i = 0$, where $q_i = p_i[(a-b)^i + (b-c)^i + (c-a)^i - 2(a+b+c)^i]$. By equation $(*)$, we conclude that $Q(t) = 0$ for all real numbers t. Hence

$$q_i = p_i[(a-b)^i + (b-c)^i + (c-a)^i - 2(a+b+c)^i] = 0 \tag{$*'$}$$

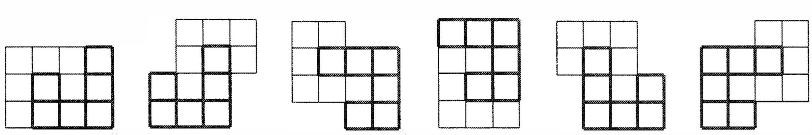
for all $0 \leq i \leq n$. In particular, if $i = 0$, then $p_i = 0$. Because $ab + bc + ca = ab + c(a+b)$, setting $a + b = 1$ and $c = -ab$ leads to good triples. Hence we consider good triples of the form $(a, b, c) = [u, (1-u), (u-1)u]$. Setting $u = 1$ and $u = 2$ in the above equation and substituting the resulting good triples into $(*')$ provides valid but limited information. (Why?) Setting $u = 3$ gives $(a, b, c) =$

$(3, -2, 6)$ and $(*')$ becomes $p_i(5^i + (-8)^i + 3^i - 2 \cdot 7^i) = 0$ for all $0 \le i \le n$. If i is odd, then $5^i + (-8)^i + 3^i - 2 \cdot 7^i = 5^i + 3^i - 8^i - 2 \cdot 7^i < 0$, and so $p_i = 0$. If i is an even integer greater than 4, then $(8/7)^i \ge (8/7)^6 = 262144/117649 > 2$, and so $5^i + (-8)^i + 3^i - 2 \cdot 7^i > 0$ and $p_i = 0$. (It is easy to check that $5^2 + 8^2 + 3^2 = 2 \cdot 7^2$ and $5^4 + 8^4 + 3^4 = 2 \cdot 7^4$.) Therefore, such polynomials have the form $P(x) = c_1x^2 + c_2x^4$ for some real numbers c_1 and c_2. We claim that any real c_1 and c_2 yield solutions of the problem. Note that if $P_1(x)$ and $P_2(x)$ are two polynomials satisfying the conditions of the problem, then $P(x) = c_1P_1(x) + c_2P_2(x)$, where c_1 and c_2 are arbitrary real numbers, is also a polynomial satisfying the conditions of the problem. Therefore, it suffices to show that $P_1(x) = x^2$ and $P_2(x) = x^4$ are indeed the solutions of the problem. We leave this process to the reader. (The case $P_2(x) = x^4$ needs a bit of work.)

3. The rectangles that can be tiled with hooks are those with sides $\{3a, 4b\}$ or $\{c, 12d\}$ with $c \notin \{1, 2, 5\}$, where $a, b, c, d \in \mathbb{Z}^+$, and the order of the dimensions is not important.

We first show that these rectangles can be tiled. We can form a 3×4 rectangle from two hooks, so we can tile any $3a \times 4b$ rectangle. In particular, we can tile $3 \times 12d$ and $4 \times 12d$ rectangles, so by joining these along their long sides, we can tile a $c \times 12d$ rectangle for any $c \ge 6$.

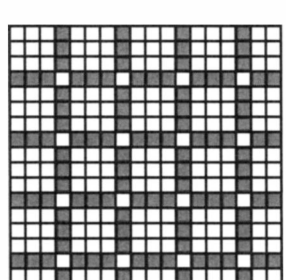
Now we show that no other rectangles can be tiled with hooks. First, note that in any tiling of a rectangle by hooks, for any hook A its center square is covered by a unique hook B of the tiling, and the center square of B must be covered by A. Hence we can pair up the hooks in a tiling, and each pair of hooks will cover one of the (unrotated) shapes shown in the figure.



(a) (c) (e) (b) (d) (f)

The upshot is that given any tiling of a rectangle with hooks, it can be uniquely interpreted as a tiling with unrotated shapes of types (a) through (f), which we shall call "chunks". In particular, the area of the rectangle must be divisible by 12, because each shape has area 12. Also, it is then clear that no rectangle with a side of length 1, 2, or 5 can be tiled by these pieces. It remains to be shown that at least one side of the rectangle must be divisible by 4.

Assume on the contrary that this is not the case; imagine the rectangle divided into unit squares, with the rows and columns formed labeled $1, \ldots, m$ and $1, \ldots, n$ (from top to bottom and from left to right). Color the square in row i and column j if exactly one of i and j is divisible by 4 (as shown here for $m = n = 18$).



Each of the six possible chunks covers 12 unit squares. Wherever they are, a straightforward verification shows that the chunk covers either 3 or 5 dark squares. Consequently, each chunk covers an *odd* number of dark squares.

Yet we can express $m = 4u + 2$, $n = 4v + 2$, so the total number of dark squares is $u(3v + 2) + v(3u + 2) = 2(3uv + u + v)$, an even number. Hence the total number of chunks is even. As in the first solution, this forces mn to be divisible by $2 \times 12 = 24$, contradicting the fact that neither is divisible by 4.

4. We lose no generality by assuming that $t_1 \le t_2 \le \cdots \le t_n$, so it suffices to show that $t_n < t_1 + t_2$. Expanding the right-hand side of the given inequality gives

$$n^2 + 1 > n + t_n\left(\frac{1}{t_1} + \frac{1}{t_2}\right) + \frac{1}{t_n}(t_1 + t_2) + \sum_{\substack{1\le i<j\le n\\(i,j)\ne(1,n),(2,n)}} \left(\frac{t_i}{t_j} + \frac{t_j}{t_i}\right).$$

By the AM-GM Inequality, $t_i/t_j + t_j/t_i \ge 2$. There are $\binom{n}{2} = \frac{n(n-1)}{2}$ pairs of integers (i, j) with $1 \le i < j \le n$. It follows that

$$n^2 + 1 > n + t_n\left(\frac{1}{t_1} + \frac{1}{t_2}\right) + \frac{1}{t_n}(t_1 + t_2) + 2\left[\binom{n}{2} - 2\right]$$

or

$$t_n\left(\frac{1}{t_1} + \frac{1}{t_2}\right) + \frac{1}{t_n}(t_1 + t_2) - 5 < 0. \qquad (*)$$

By the AM-GM Inequality, $(t_1 + t_2)(1/t_1 + 1/t_2) = 2 + t_1/t_2 + t_2/t_1 \ge 4$, and so $4t_n(t_1 + t_2) \le t_n(1/t_1 + 1/t_2)$. Substituting the last inequality into inequality $(*)$ gives

$$\frac{4t_n}{t_1 + t_2} + \frac{1}{t_n}(t_1 + t_2) - 5 < 0.$$

Setting $(t_1 + t_2)/t_n = x$ in the last equality yields $4/x + x - 5 < 0$, or $0 > x^2 - 5x + 4 = (x - 1)(x - 4)$. It follows that $1 < x < 4$, that is, $t_n < t_1 + t_2 < 4t_n$, which implies the desired result. (Note: The upper bound $n^2 + 1$ can be improved to $(n + \sqrt{10} - 3)^2$.)

5. Let ω' be the circumcircle of triangle BCD. Extend segments BP and DP through P to meet ω' again at E and F, respectively. Because $BFCE$ is cyclic, $\angle EFC = \angle EBC = \angle PBC = \angle ABD$. Likewise, $\angle FEC = \angle ADB$. Hence triangles ABD and CFE are similar, with ratio BD/EF. Because $BDFE$ is cyclic, triangles BDP and FEP are similar, with ratio BD/FE. It follows that quadrilaterals $ABPD$ and $CFPE$ are similar.

Therefore, $AP = CP$ if and only if quadrilaterals $ABPD$ and $CFPE$ are congruent, or $BD = EF$. Hence $AP = CP$ if and only if $\angle BFD = \angle EDF$. Because triangles ABD and CFE are similar, $\angle DAB = \angle ECF$. Because $DECF$ is cyclic, $AP = CP$ if and only if $\angle DAB + \angle BFD = \angle ECF + \angle EDF = 180°$; that is, if and only if $ABFD$ is cyclic. It follows that $AP = CP$ if and only if $ABFCED$ is cyclic.

6. The answers are those positive integers that are not divisible by 20. We call an integer n an *alternator* if it has a multiple which is alternating. Because any multiple of 20 ends with an even digit followed by 0, multiples of 20 are not alternating. Hence multiples of 20 are not alternators. We claim that all other positive integers are alternators. Let n be positive integer not a multiple of 20. Note that all divisors of an alternator are alternators. We may assume that n is a even number. We establish

the following fact: If $n = 2^\ell$ or $2 \cdot 5^\ell$, for some positive integer ℓ, then there exists a multiple $X(n)$ of n such that $X(n)$ is alternating and $X(n)$ has n digits. Indeed, set

$$M = \frac{10^{n+1} - 10}{99} = \overline{\underbrace{101010\ldots10}_{n \text{ digits}}}.$$

For every integer $k = 0, 1, \ldots, n-1$, there exists a sequence $e_0, e_1, \ldots, e_k \in \{0, 2, 4, 6, 8\}$ such that $M + \sum_{i=0}^{k} e_i \cdot 10^i$ is divisible by 2^{k+2} if n is of the form 2^ℓ, or by $2 \cdot 5^{k+1}$ if $n = 2 \cdot 5^\ell$. This is straightforwardly proved by induction on k. In particular, there exist $e_0, \ldots, e_{n-1} \in \{0, 2, 4, 6, 8\}$ such that

$$X(n) = M + \sum_{i=0}^{k} e_i \cdot 10^i$$

is divisible by n. This $X(n)$ is alternating and has n digits, establishing our claim.

Because n is even and not divisible by 20, we write n in the form $n'm$, where $n' = 2^\ell$ or $2 \cdot 5^\ell$ and $\gcd(m, 10) = 1$. Let $c \geq n'$ be an integer such that $10^c \equiv 1 \pmod{m}$. (Such a c exists because $10^{\varphi(m)} \equiv 1 \pmod{m}$.) Let

$$M = \frac{10^{2mc+1} - 10}{99} \cdot 10^{n'} + X(n') = \overline{\underbrace{101010\ldots10}_{2mc \text{ digits}} X(n')}.$$

There exists $k \in \{0, 1, 2, \ldots, m-1\}$ such that $M \equiv -2k \pmod{m}$. Then $X(n) = M + \sum_{i=1}^{k} 2 \cdot 10^{ci}$ is divisible by m. This $X(n)$ is also divisible by n' (as n' divides $10^{n'}$, which divides 10^c) and is alternating. Thus n is an alternator.

2004 Olympiad Results

The top twelve students on the 2004 USAMO were (in alphabetical order):

Jae Bae	Academy of Advancement in Science and Technology	Hackensack, NJ
Jongmin Baek	Cupertino High School	Cupertino, CA
Oleg Golberg	Homeschooled	Exeter, NH
Matt Ince	St. Louis Family Church Learning Center	Chesterfield, MO
Janos Kramar	University of Toronto Schools	Toronto, ON
Tiankai Liu	Phillips Exeter Academy	Exeter, NH
Alison Miller	Home Educators Enrichment Group	Niskayuna, NY
Aaron Pixton	Vestal Senior High School	Vestal, NY
Brian Rice	Southwest Virginia Governor's School	Dublin, VA
Jacob Tsimerman	University of Toronto Schools	Toronto, ON
Ameya Velingker	Parkland High School	Allentown, PA
Tony Zhang	Phillips Exeter Academy	Exeter, NH

Tiankai Liu, with a perfect score, was the winner of the Samuel Greitzer-Murray Klamkin award, given to the top scorer(s) on the USAMO. Tiankai is the winner of this award for the third year in a row. Tiankai Liu, Oleg Golberg, and Tony Zhang placed first, second, and third, respectively, on the USAMO. They were awarded college scholarships of \$15000, \$10000, and \$5000, respectively, by the Akamai Foundation. The Clay Mathematics Institute (CMI) award, for a solution of outstanding elegance, and carrying a \$3000 cash prize, was presented to Matt Ince for his solution to USAMO Problem 2.

The USA team members were chosen according to their combined performance on the 33rd annual USAMO, and the Team Selection Test that took place at the Mathematical Olympiad Summer Program (MOSP), held at the University of Nebraska–Lincoln, June 13–July 3, 2004. Members of the USA team at the 2004 IMO (Athens, Greece) were Oleg Golberg, Matt Ince, Tiankai Liu, Alison Miller, Aaron Pixton, and Tony Zhang. Zuming Feng (Phillips Exeter Academy) and Po-Shen Loh (California Institute of Technology) served as team leader and deputy leader, respectively. The team was also accompanied by Reid Barton (Massachusetts Institute of Technology), Zvezdelina Stankova (Mills College), and Steven Dunbar (University of Nebraska-Lincoln), as observers of the team leader and deputy leader, respectively. During the competition, Professor Edward Witten (Institute for Advanced Study in Princeton, Fields medal winner) visited the team and congratulated the team's performance.

At the 2004 IMO, gold medals were awarded to students scoring between 32 and 42 points, silver medals to students scoring between 24 and 31 points, and bronze medals to students scoring between 16 and 23 points. There were 45 gold medalists, 78 silver medalists, and 120 bronze medalists. There were 4 perfect papers (Tsimerman from Canada, Rácz from Hungary, and Badzyan and Dubashinskiy from the Russian Federation) on this difficult exam. Golberg's score of 40 tied for 7th place overall. Miller became the first female gold medalist from our country. The team's individual performances were as follows:

Golberg	GOLD Medalist	Liu	GOLD Medalist
Ince	SILVER Medalist	Pixton	GOLD Medalist
Miller	GOLD Medalist	Zhang	GOLD Medalist

The total team scores on the first five problems were all even for the top three teams, namely, China, USA, and Russian Federation. Therefore, the total team scores (China 42, USA 34, and Russia 27) on the sixth problem become the deciding factor of the team rankings. In terms of total score (out of a maximum of 252), the highest ranking of the 85 participating teams were as follows:

China	220	Vietnam	196	Hungary	187	Romania	176
USA	212	Bulgaria	194	Japan	182	Ukraine	174
Russia	205	Taiwan	190	Iran	177	Korea	166

The 2004 USAMO was prepared by Titu Andreescu (Chair), Steven Dunbar, Zuming Feng, Kiran Kedlaya, Alexander Soifer, Richard Stong, Zoran Šunić, Zvezdelina Stankova, and David Wells. The Team Selection Test was prepared by Titu Andreescu and Zuming Feng. The MOSP was held at the University of Nebraska-Lincoln. Thanks to a generous grant from the Akamai Foundation, the 2004 MOSP expanded from the usual 24–30 students to 54 with an appropriate number of instructors and assistants. Zuming Feng (Academic Director), Titu Andreescu, Chris Jeuell, Qin Jing, Po-Shen Loh, Alex Saltman, and Zvezdelina Stankova served as instructors, assisted by Reid Barton as junior instructor, and Mark Lipson, Ricky Liu, Po-Ru Loh, Gregory Price, and Inna Zakharevich as graders. Steven Dunbar (MOSP Director) and Kiran Kedlaya served as guest instructors.

For more information about the USAMO or the MOSP, contact Steven Dunbar at `sdunbar@math.unl.edu`.

CONTENTS

ARTICLES

NOTES

PROBLEMS

REVIEWS

NEWS AND LETTERS

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, DC 20036