MATHEMATICS MAGAZINE

CONTENTS

VOLUME 38 • JANUARY 1965 • NUMBER 1

MATHEMATICS MAGAZINE

ROY DUBISCH, *Editor*

EDITORIAL CORRESPONDENCE should be sent to the Editor, ROY DUBISCH, Department of Mathematics, University of Washington, Seattle, Washington 98105. Articles should be typewritten and double-spaced on $8\frac{1}{2}$ by 11 paper. The greatest possible care should be taken in preparing the manuscript, and authors should keep a complete copy. Figures should be drawn on separate sheets in India ink and of a suitable size for photographing.

NOTICE OF CHANGE OF ADDRESS and other subscription correspondence should be sent to the Executive Director, H. M. GEHMAN, Mathematical Association of America SUNY at Buffalo (University of Buffalo), Buffalo, New York 14214.

ADVERTISING CORRESPONDENCE should be addressed to F. R. OLSON, Mathematical Association of America, SUNY at Buffalo (University of Buffalo), Buffalo, New York 14214.

The MATHEMATICS MAGAZINE is published by the Mathematical Association of America at Buffalo, New York, bi-monthly except July-August. Ordinary subscriptions are: 1 year \$3.00; 2 years \$5.75; 3 years \$8.50; 4 years \$11.00; 5 years \$13.00. Members of the Mathematical Association of America may subscribe at the special rate of 2 years for \$5.00. Single copies are 65¢.

PUBLISHED WITH THE ASSISTANCE OF THE JACOB HOUCK MEMORIAL FUND OF THE MATHEMATICAL ASSOCIATION OF AMERICA

Second class postage paid at Buffalo, New York and additional mailing offices.

COMPLETE RESIDUE SYSTEMS IN THE GAUSSIAN INTEGERS

J. H. JORDAN AND C. J. POTRATZ, Washington State University

1. As a matter of notation small case Latin letters will represent real integers and Greek letters will represent Gaussian integers.

There are many representations for the complete residue system modulo n but the one that usually comes to mind is the set of integers $\{0, 1, 2, \cdots, n-1\}$. Other representations are sometimes used; for example if $(a, n)=1$ then $\{a, 2a, 3a, \cdots, na\}$ is a representation of the complete residue system modulo n. Another representation which has a somewhat pleasing quality is found in Uspensky and Heaslet [1] and is $\{x \mid -n/2<x\leqq n/2\}$ which is the representation with least absolute values.

Consider the meaning of divisibility and congruences in the Gaussian integers. Recall that in the Gaussian integers $\gamma \mid \beta$ means there is a Gaussian integer α such that $\alpha\cdot\gamma=\beta$, and $\alpha\equiv\beta \pmod{\gamma}$ means that $\gamma \mid \alpha-\beta$. This congruence relation is an equivalence relation and, analogous to the real case, it is reasonable to define the complete residue system modulo γ as the set of equivalence classes formed from the Gaussian integers with respect to the principal ideal (γ). The complete residue system modulo γ will be abbreviated as CRS (mod γ). Without any loss of generality γ can be restricted to being in the first quadrant or on the positive real line.

It is the purpose of this paper to exhibit several representations for the CRS (mod γ). These representations are given in section 2 and the verification that they are representations of the complete residue systems is given in section 3.

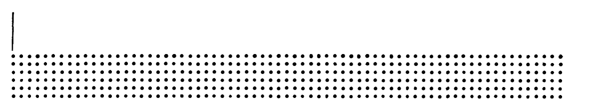


FIG. 1. CRS (mod $21+7i$).

2. The first representation of CRS (mod γ), $\gamma=a+bi$, seems to be a natural generalization of $\{0, 1, 2, \cdots, n-1\}$ modulo n.

REPRESENTATION A. If $d=(a, b)$ so that $\gamma=d(a_1+b_1i)$ then $T=\{x+yi \mid 0\leqq x \leqq d(a_1^2+b_1^2)-1, 0\leqq y\leqq d-1\}$ is a representation of CRS (mod γ), (see Figure 1).

The set T is a rectangular set of points with vertices $(0, 0)$, $(0, d-1)$, $(d(a_1^2+b_1^2)-1, d-1)$, and $(d(a_1^2+b_1^2)-1, 0)$.

The second type of representation for the CRS (mod γ) is called a Utah representation and is as follows:

REPRESENTATION B. Let s and t be arbitrary,

$$A = \{x + yi \mid s \leqq x \leqq s + a - 1, t \leqq y \leqq t + a - 1\} \text{ and}$$
$$B = \{x + yi \mid s + a \leqq x \leqq s + a + b - 1, t \leqq y \leqq t + b - 1\}$$

then $A\cup B$ is a representation of the CRS (mod γ), (see Figures 2 and 3).

The shape of this array is somewhat indicated by the name Utah.

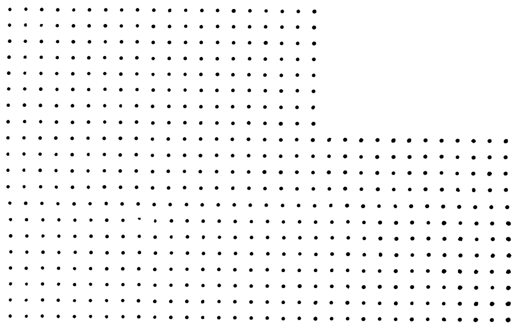


FIG. 2. CRS (mod $20+12i$).

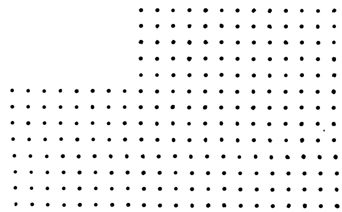


FIG. 3. CRS (mod $8+13i$).

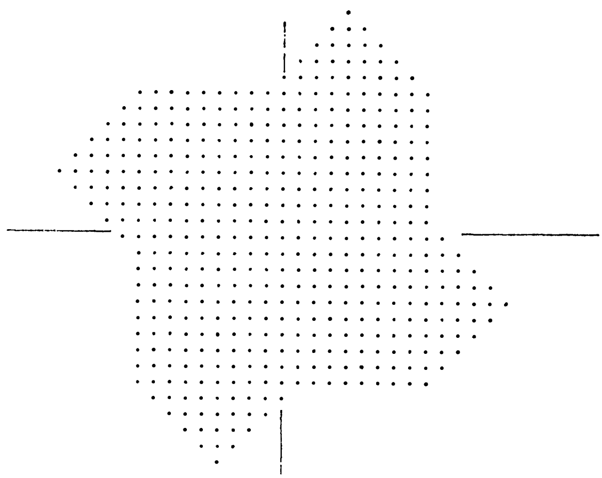


FIG. 4. CRS (mod $19+10i$).

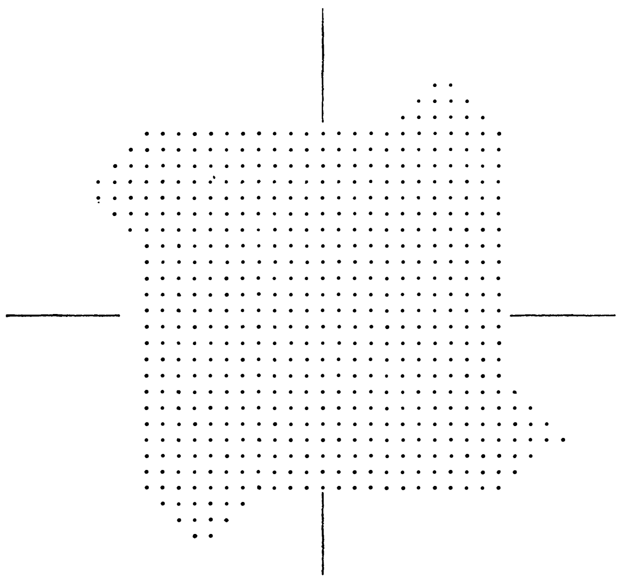


FIG. 5. CRS (mod $23+7i$).

In order to generalize the representation of the complete residue system modulo n with least absolute values it is helpful to consider these preliminaries:

DEFINITION 1. *A representation R, of the CRS* (mod γ) *is called "best" if for any representation T of the CRS* (mod γ) *there is an $\alpha \in T$ such that $|\alpha| \geqq |\beta|$ for all $\beta \in R$.*

There are usually many "best" representations for a given modulus and some of these might be considered "better" in certain ways, for example a representation R might be considered "better" than a representation T if $\sum_{\beta\in R} |\beta| < \sum_{\alpha\in T} |\alpha|$. This paper will not be concerned with a hierarchy of "best" representations but will just be concerned with exhibiting a "best" representation for every γ.

In order to simplify notation consider the following:

DEFINITION 2. *If S is a set of Gaussian integers and α and β are Gaussian integers, then $\alpha S \oplus \beta = \{\alpha\delta + \beta \mid \delta \in S\}$.*

The set $\alpha S \oplus \beta$ is a rotation, magnification, and translation of the set S.

The third type of representation is a "best" representation and is as follows:

REPRESENTATION C. Let $a \geqq b \geqq 0$.

Case 1. If $a = 2n+1$, $b = 2m$,

$$A = \{x + yi \mid -n \leqq x \leqq n,\ -n \leqq y \leqq n\} \text{ and}$$
$$B = \{x + yi \mid n + 1 \leqq x \leqq n + m,\ x - a + 1 \leqq y \leqq b - x\},$$

then $A \cup B \cup (iB) \cup (-B) \cup (-iB)$ is a "best" representation of CRS (mod γ). (See Figure 4.)

Case 2. If $a = 2n+1$, $b = 2m+1$, A and B are as in case 1, and $P = \{n+m+1-(n-m)i\}$, then $A \cup B \cup (iB) \cup (-B) \cup (-iB) \cup P$ is a "best" representation of the CRS (mod γ). (See Figure 5.)

Case 3. If $a = 2n$, $b = 2m$,

$$A = \{x + yi \mid -n \leqq x \leqq n - 1,\ -n + 1 \leqq y \leqq n\} \text{ and}$$
$$B = \{x + yi \mid n \leqq x \leqq n + m - 1,\ x - a + 2 \leqq y \leqq b - x\},$$

then $A \cup B \cup (iB + i) \cup (-B - 1 + i) \cup (-iB - 1)$ is a "best" representation of the CRS (mod γ). (See Figure 6.)

Case 4. If $a = 2n$, $b = 2m+1$, A as in case 3,

$$B = \{x + yi \mid n \leqq x \leqq n + m,\ x - a + 2 \leqq y \leqq b - x + 1\} \text{ and}$$
$$C = \{x + yi \mid n + 1 \leqq y \leqq n + m,\ y - b + 1 \leqq x \leqq a - y + 1\},$$

then $(A - \{-n+ni\}) \cup B \cup -iB \cup C \cup iC$ is a "best" representation of the CRS (mod γ). (See Figure 7.)

In cases where $b > a > 0$ the roles of the x's and y's would be changed in each of these representations and the results would be a mirror image of the above representations. (See Figures 8, 9, 10, and 11.)

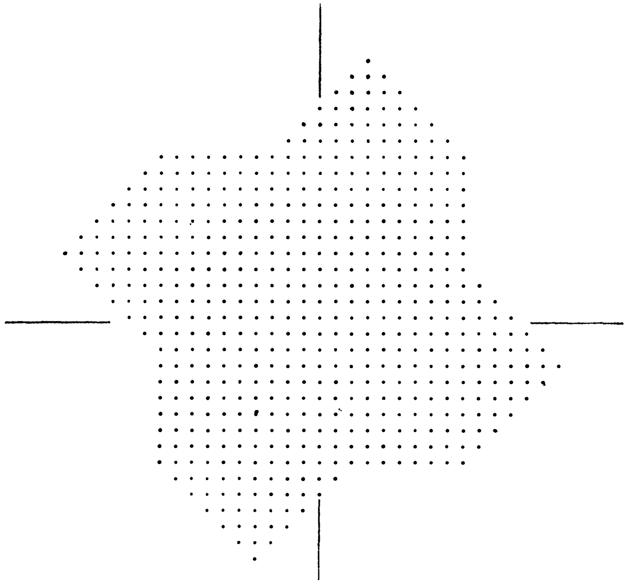


FIG. 6. CRS (mod $20+12i$).

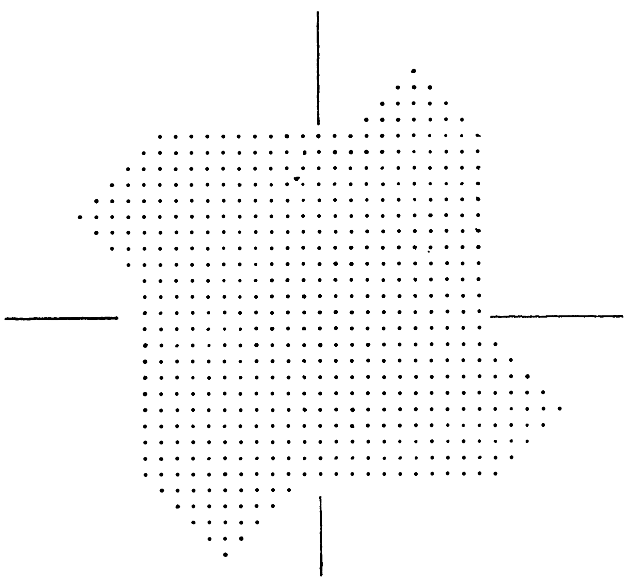


FIG. 7. CRS (mod $22+9i$).

The last representation exhibited is a representation generated from given representations and is as follows:

REPRESENTATION D. If R_1 and R_2 are representations of the CRS (mod γ) and the CRS (mod δ) respectively, then $P=\bigcup_{\alpha\in R_2}(\delta R_1\oplus\alpha)$ is a representation of the CRS (mod $\gamma\delta$). (See Figure 12.)

Unfortunately, the representation generated from two "best" representations is not necessarily a "best" representation.

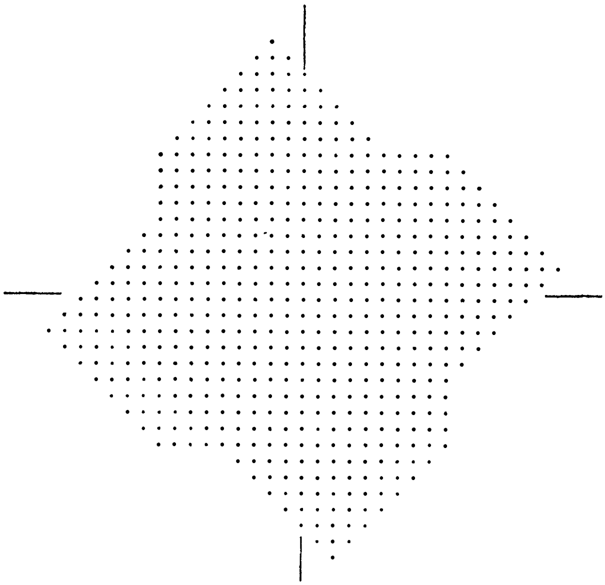


FIG. 8. CRS (mod $14+19i$).

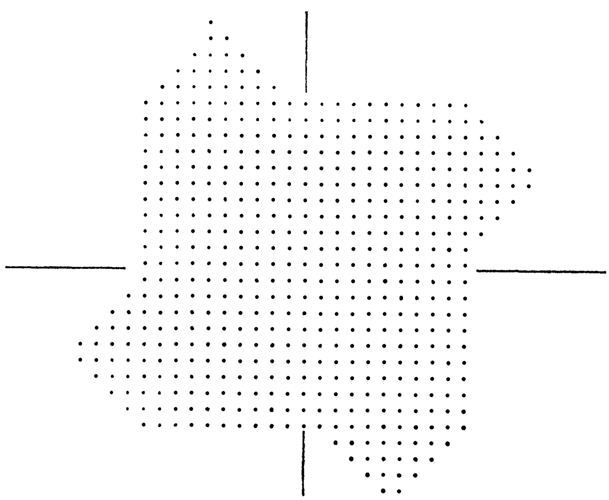


FIG. 9. CRS (mod $9+21i$).

3. Verifications.

REPRESENTATION A. To verify that the elements of representation A form a CRS (mod γ), let $\alpha_1=x_1+y_1i$ and $\alpha_2=x_2+y_2i$ be any elements of representation A. If $\alpha_1\equiv\alpha_2$ (mod γ), then $d\mid\alpha_2-\alpha_1$; hence $d\mid y_2-y_1$. But $|y_2-y_1|<d$; hence $y_2=y_1$. Now $\gamma\mid x_2-x_1$; but the smallest real integer that γ divides is $d(a_1^2+b_1^2)$ so either $|x_2-x_1|\geqq d(a_1^2+b_1^2)$ or $x_2=x_1$. Since the first of these is impossible by the definition of representation A, the latter must hold so $\alpha_1=\alpha_2$. Therefore distinct elements of representation A are incongruent modulo γ.

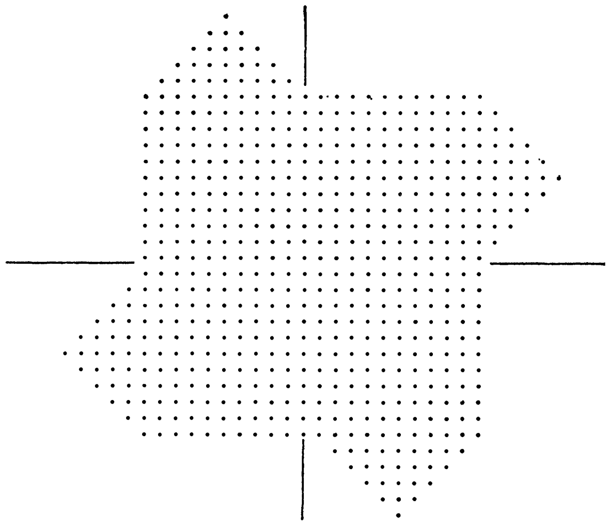


FIG. 10. CRS (mod $10+22i$).

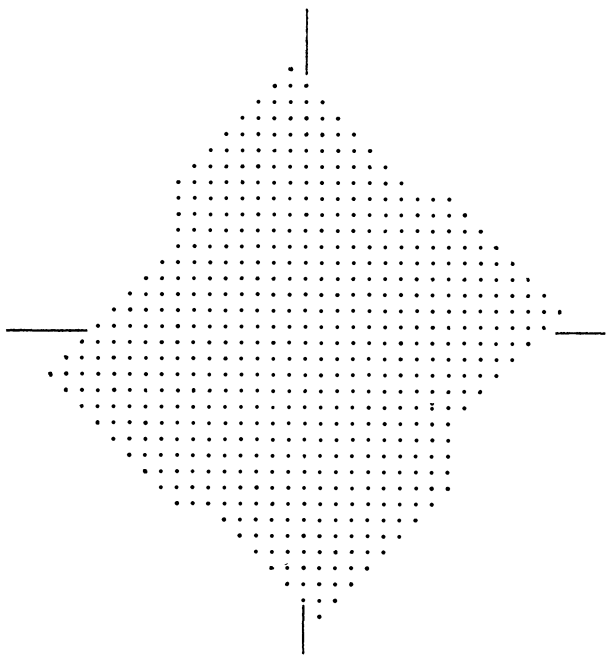


FIG. 11. CRS (mod $15+18i$).

Consider an arbitrary Gaussian integer, $\beta = x+yi$. Now determine q_1 and r so that $y = dq_1 + r$, where $0 \leqq r < d$. Since $(a, b) = d$ there are integers u and v such that $av + bu = dq_1$. Now

$$x + yi - (a + bi)(u + vi) = x - au + bv + ri.$$

Determine q_2 and s so that $x - au + bv = d(a_1^2 + b_1^2)q_2 + s$, $0 \leqq s < d(a_1^2 + b_1^2)$. Now

$$x + yi - (a + bi)(u + vi + q_2(a_1 - b_1 i)) = s + ri;$$

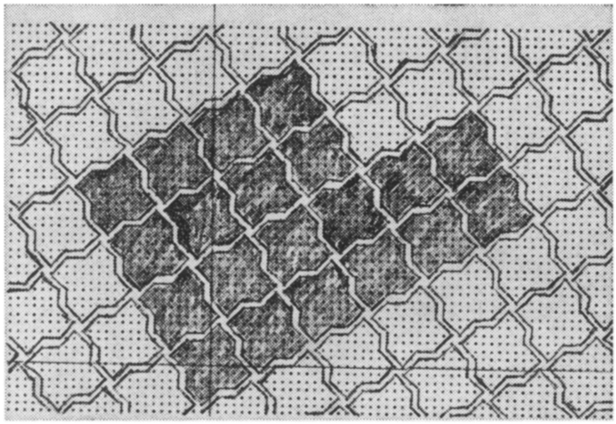


FIG. 12. CRS (mod $(7+4i)(4+2i)$), where R_1 is a "best" and R_2 is a Utah.

that is $x+yi\equiv s+ri \pmod{\gamma}$, $0\leqq s<d(a_1^2+b_1^2)$ and $0\leqq r<d$. Hence any Gaussian integer is congruent to an element of representation A; therefore representation A is a CRS (mod γ).

COROLLARY. *The cardinality of the CRS* (mod γ) *is* $|\gamma|^2=a^2+b^2=d^2(a_1^2+b_1^2)$.

REPRESENTATION B (*Utah*). The cardinality of the lattice points in the Utah representation is a^2+b^2, so it will suffice to show that two distinct elements of the Utah representation are incongruent modulo γ.

Let $\alpha_1=x_1+y_1i$ and $\alpha_2=x_2+y_2i$ be two points in a Utah representation. If $\alpha_1\equiv\alpha_2 \pmod{\gamma}$ then there is a δ such that

$$\gamma\delta = \alpha_2 - \alpha_1 = x_2 - x_1 + (y_2 - y_1)i.$$

Now by the definition of the Utah representation and if $a\geqq b$, then $|x_2-x_1|\leqq a+b-1$ and $|y_2-y_1|\leqq a-1$. So it must be that

$$\begin{aligned} |\delta|^2 = \frac{|\alpha_2-\alpha_1|^2}{|\gamma|^2} &\leqq \frac{(a+b-1)^2+(a-1)^2}{a^2+b^2} \\ &= \frac{a^2+b^2+2ab-4a-2b+a^2+2}{a^2+b^2} \\ &< 1+\frac{2ab}{a^2+b^2}+\frac{a^2}{a^2+b^2}+\frac{2}{a^2+b^2} \\ &\leqq 4+\frac{2ab}{a^2+b^2} = 4+\frac{2}{\dfrac{a}{b}+\dfrac{b}{a}}\,. \end{aligned}$$

If $b>0$, then $a/b+b/a\geqq 2$ so $|\delta|^2<5$; if $b=0$, then $|\delta|^2<4$. Thus the only admissible values for δ are 0, ± 1, $\pm i$, ± 2, $\pm 2i$ and $\pm 1\pm i$. If $a<b$ the same result is obtained.

Now $\gamma\delta+\alpha_1=\alpha_2$ is not solvable for these δ's unless $\delta=0$; therefore any two distinct elements of a Utah representation are incongruent modulo γ.

REPRESENTATION C. It suffices to show that a representation C can be obtained from a specific Utah representation of the CRS (mod γ).

Let U_{2n+1} be the Utah representation of the CRS (mod γ), where $\gamma=2n+1+bi$, with $t=s=-n$, and let U_{2n} be the Utah representation of the CRS (mod γ), where $\gamma=2n+bi$ with $t=1-n$ and $s=-n$.

In U_{2n+1} set B can be described as

$$\{x+yi \mid n+1 \leqq x \leqq n+b,\ -n \leqq y \leqq b-n+1\}.$$

In U_{2n} set B can be described as

$$\{x+yi \mid n \leqq x \leqq n+b-1,\ 1-n \leqq y \leqq b-n\}.$$

Case 1. $a=2n+1$, $b=2m$. Separate the B of U_{2n+1} into four disjoint subsets as follows:

$$C_1 = \{x+yi \mid n+1 \leqq x \leqq n+m,\ x-a+1 \leqq y \leqq b-x-1\},$$
$$C_2 = \{x+yi \mid -n \leqq y \leqq -n+m-1,\ y+a \leqq x \leqq b-1-y\},$$
$$C_3 = \{x+yi \mid n+m+1 \leqq x \leqq n+b,\ b-x \leqq y \leqq x-a-1\}, \text{ and}$$
$$C_4 = \{x+yi \mid -n+m \leqq x \leqq b-n-1,\ b-y+1 \leqq x \leqq y+a\}.$$

(See Figure 13.)

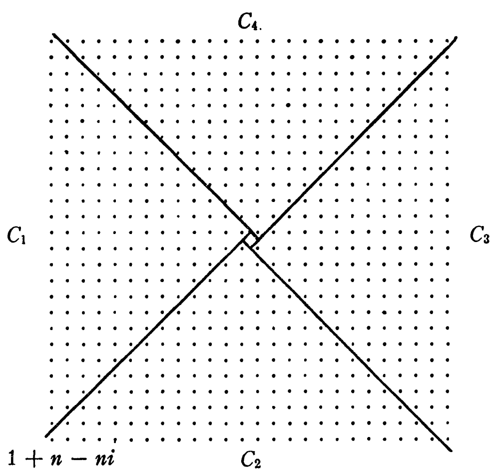


FIG. 13.

Case 1 of representation C can now be described as

$$A \cup C_1 \cup C_2 \oplus i\gamma \cup C_3 \oplus (i-1)\gamma \cup C_4 \oplus (-\gamma).$$

Since each component of this union is point for point congruent to the corresponding subset of the Utah representation and the cardinalities agree, case 1 is a representation of the CRS (mod γ).

To show that it is a "best" representation consider $(n+m)+(m-n)i$, the vertex of C_1. Now

$$\left| n + m + (m - n)i \right| = \sqrt{2}\sqrt{(m^2 + n^2)} < \frac{\sqrt{2}}{2} \sqrt{(a^2 + b^2)}.$$

If $x+yi \equiv (m+n)+(m-n)i \pmod{\gamma}$, then

$$\text{(I)} \qquad \gamma\mu + (m + n) + (m - n)i = x + yi.$$

Hence

$$\begin{aligned} \left| x + yi \right| &\geqq \left| \gamma\mu \right| - \sqrt{2}\sqrt{(m^2 + n^2)} \\ &> \left| \mu \right| \sqrt{(a^2 + b^2)} - \frac{\sqrt{2}}{2} \sqrt{(a^2 + b^2)} \\ &= \left(\left| \mu \right| - \frac{\sqrt{2}}{2} \right) \sqrt{(a^2 + b^2)}. \end{aligned}$$

If $|\mu| \geqq \sqrt{2}$, then $|x+yi| > |(m+n)+(m-n)i|$. If $|\mu| < \sqrt{2}$, then $\mu = 0, \pm 1$, or $\pm i$. Checking (I) for these values, one easily establishes that $|m+n+(m-n)i| < |x+yi|$ unless $\mu = 0$ or, in other words, $m+n+(m-n)i$ is the element of its residue class modulo γ with least absolute value. The vertices of the other four triangles have the same absolute value as $m+n+(m-n)i$ and the corners of the square A have absolute value $\sqrt{2}\, n$ which is at least as small as $\sqrt{2}\sqrt{(m^2+n^2)}$; hence $|x+yi| \leqq |(m+n)+(m-n)i|$ for all $x+yi$ in this representation. Therefore case 1 is a "best" representation of the CRS $\pmod{\gamma}$.

Case 2. $a = 2n+1$, $b = 2m+1$. Separate the B of U_{2n+1} into four disjoint subsets as follows:

$$\begin{aligned} D_1 &= \{x + yi \mid n + 1 \leqq x \leqq n + m,\ x - a + 1 \leqq y \leqq b - x\} \\ &\quad \cup \{n + m + 1 + (m - n)i\}, \\ D_2 &= \{x + yi \mid -n \leqq y \leqq -n + m - 1,\ y + a \leqq x \leqq b - 1 - y\}, \\ D_3 &= \{x + yi \mid n + m + 2 \leqq x \leqq n + b,\ b - x \leqq y \leqq x - a - 1\}, \text{ and} \\ D_4 &= \{x + yi \mid -n + m + 1 \leqq y \leqq b - 1 - n,\ b - y + 1 \leqq x \leqq y + a\}. \end{aligned}$$

(See Figure 14.)

Case 2 of representation C can now be described as

$$A \cup D_1 \cup D_2 \oplus i\gamma \cup D_3 \oplus (i - 1)\gamma \cup D_4 \oplus (-\gamma).$$

Since each component of this union is point for point congruent to the corresponding subset of the Utah representation and the cardinality is the same, case 2 is a representation of the CRS $\pmod{\gamma}$.

To show that it is a "best" representation, consider $n+m+1+(m-n)i$, the vertex of D_1. Now

$$\left| m + n + 1 + (m - n)i \right| = \sqrt{2}\sqrt{(m^2 + n^2 + m + n + \tfrac{1}{2})} = \frac{\sqrt{2}}{2} \sqrt{(a^2 + b^2)}.$$

If $x+yi=(m+n+1)+(m-n)i+\gamma\mu$ and if $|\mu|>\sqrt{2}$ then, as before,

$$|x+yi| > \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)} = |m+n+1+(m-n)i|.$$

On the other hand, if $|\mu|\leqq\sqrt{2}$, that is $\mu=0$, ± 1, $\pm i$ or $\pm 1\pm i$, the inequality $|x+yi|\geqq|m+n+1+(m-n)i|$ holds for all these values and equality actually exists for $\mu=0$, i, -1, and $i-1$. Therefore, $m+n+1+(m-n)i$ is an element of its residue class with as small an absolute value as possible. Further, if $x+yi$ is any other point in representation C, then the inequality $|x+yi|<|m+n+1+(m-n)i|$ holds. Hence case 2 is a "best" representation of CRS (mod γ).

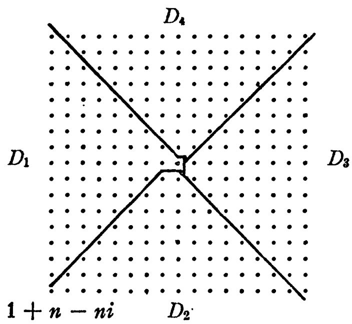


FIG. 14.

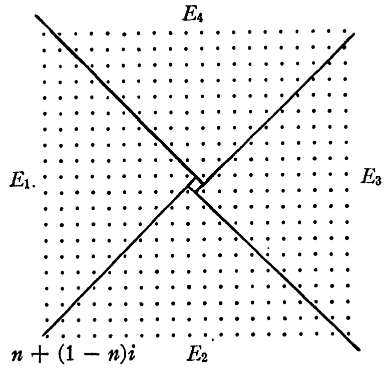


FIG. 15.

Case 3. $a=2n$, $b=2m$. Separate the B of U_{2n} into four disjoint subsets as follows:

$$E_1 = \{x+yi \mid n\leqq x\leqq n+m-1,\ x-a+2\leqq y\leqq b-x\},$$
$$E_2 = \{x+yi \mid 1-n\leqq y\leqq m-n,\ y+a-1\leqq x\leqq b-1-y\},$$
$$E_3 = \{x+yi \mid n+m\leqq x\leqq n+b-1,\ b-x\leqq y\leqq x-a\}, \text{ and}$$
$$E_4 = \{x+yi \mid m-n+1\leqq y\leqq -n+b,\ b-y+1\leqq x\leqq y+a-1\}.$$

(See Figure 15.)

Case 3 of representation C can now be described as $A\cup E_1\cup E_2\oplus i\gamma \cup E_3\oplus(i-1)\gamma\cup E_4\oplus(-\gamma)$. Since each component of this union is point for point congruent to the corresponding subset of the Utah representation and the cardinality is the same, case 3 is a representation of the CRS (mod γ).

To show that it is a "best" representation, consider point $-n-m+(n-m)i$, the vertex of $E_3\oplus(i-1)\gamma$. Now

$$|-n-m+(n-m)i| = \sqrt{2}\sqrt{(n^2+m^2)} = \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)}.$$

Now if $x+yi=-n-m+(n-m)i+\gamma\mu$ with $|\mu|>\sqrt{2}$, then

$$\begin{aligned} |x+yi| &> \sqrt{2}\sqrt{(a^2+b^2)} - |-n-m+(n-m)i| \\ &= \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)} = |-n-m+(n-m)i|. \end{aligned}$$

For $|\mu| \leqq \sqrt{2}$ or $\mu=0, \pm 1, \pm i$, or $\pm 1 \pm i$, the inequality also holds except when $\mu=0, -i, 1$, and $1-i$ and in these cases equality holds. Further if $x+yi$ is in case 3 of representation C then $|x+yi| \leqq |-n-m+(n-m)i|$. Therefore case 3 is a "best" representation of CRS (mod γ).

Case 4. $a=2n$, $b=2m+1$. Separate the B of U_{2n} into four disjoint subsets as follows:

$$\begin{aligned} F_1 &= \{x+yi \mid n \leqq x \leqq n+m,\ x-a+1 \leqq y \leqq b-x\}, \\ F_2 &= \{x+yi \mid 1-n \leqq y \leqq m-n,\ y+a \leqq x \leqq b-y-1\}, \\ F_3 &= \{x+yi \mid n+m+1 \leqq x \leqq n+b-1,\ b-x \leqq y \leqq x-a-1\}, \text{ and} \\ F_4 &= \{x+yi \mid m-n+1 \leqq y \leqq b-n,\ b-y+1 \leqq x \leqq y+a\} \\ &\quad - \{n+b+(b-n)i\}. \end{aligned}$$

(See Figure 16.)

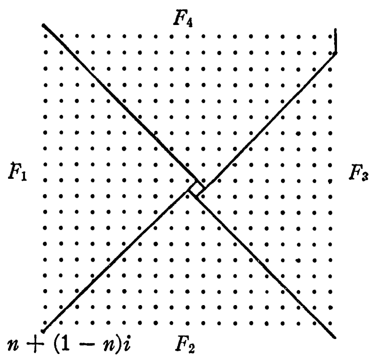


FIG. 16.

Case 4 of representation C can now be described as

$$A-\{-n+ni\}\cup F_1\cup F_2\oplus(i\gamma)\cup F_3\oplus(i-1)\gamma\cup F_4+(-\gamma)\cup\{-n+b+ni\}.$$

Since each component of this union is point for point congruent to the corresponding subsets of the Utah representation and the cardinality is the same, case 4 is a representation of the CRS (mod γ).

To show that it is a "best" representation, consider point $(n+m)+(m-n+1)i$, the vertex of F_1. Now

$$|n+m+(m-n+1)i| = \sqrt{2}\sqrt{(n^2+m^2-n+m+1/2)} < \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)}.$$

If $x+yi=n+m+(m-n+1)i+\gamma\mu$ with $|\mu| \geqq \sqrt{2}$ then

$$|x+yi| > \sqrt{2}\sqrt{(a^2+b^2)} - \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)}$$
$$= \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)} > |n+m+(m-n+1)i|.$$

If $|\mu| < \sqrt{2}$ or $\mu = 0, \pm 1$, or $\pm i$ the same inequality holds unless $\mu = 0$. It can also be shown that for $x+yi$ in case 4, $|x+yi| \leqq |n+m+(m-n+1)i|$ and equality will hold for

$$x+yi = -n-m+(n-m-1)i, \quad -n+m+1+(-n-m)i, \text{ or}$$
$$n-m-1+(n+m)i$$

all of which are vertices of the other three triangles. Therefore the representation is a "best" representation.

Notice that it was necessary to put the upper left hand corner point $-n+ni$ at point $-n+b-ni$ to take care of the cases where $n > 2m^2+2m+1$.

REPRESENTATION D. Since the components of $P = \bigcup_{\alpha \in R_2} (\delta R_1 \oplus \alpha)$ are disjoint and the cardinality of each $\delta R_1 \oplus \alpha = |\gamma|^2$, the cardinality of P is $|\gamma|^2 |\delta|^2 = |\gamma\delta|^2$, i.e., just the proper size to be a representation of the CRS (mod $\gamma\delta$). If $\xi_1 = \delta\beta_1 + \alpha_1$ and $\xi_2 = \delta\beta_2 + \alpha_2$ are elements of P and if $\delta\beta_1 + \alpha_1 \equiv \delta\beta_2 + \alpha_2$ (mod $\gamma\delta$), then $\alpha_1 \equiv \alpha_2$ (mod δ) or $\alpha_1 = \alpha_2$ since both α_1 and α_2 are in R_2. Further, if $\gamma\delta | \delta(\beta_1 - \beta_2)$, then $\gamma | \beta_1 - \beta_2$; thus $\beta_1 = \beta_2$ since β_1 and β_2 are both in R_1. Thus distinct elements of P are incongruent modulo $\gamma\delta$ and therefore P is a representation of the CRS (mod $\gamma\delta$).

Reference

1. J. V. Uspensky and M. A. Heaslet, Elementary number theory, McGraw-Hill, New York, 1939.

A NOTE ON PRIMITIVE ROOTS

JOHN D. BAUM, Oberlin College

In teaching a one semester course in elementary number theory, the author has found that it is usually possible to finish the course by discussing quadratic reciprocity and a few of its consequences. The results which follow hang together in a mathematically esthetic fashion, utilize some of the results of quadratic reciprocity, and make some contribution to the theory of primitive roots. A cursory search of the literature reveals that at least one of these results (Theorem 1) appears not to be mentioned elsewhere, while others (Theorem 2) appear to be known. (Cf. [1] p. 127, Ex. 75 and 76, or [2], p. 122, Ex. 5.)

$$|x+yi| > \sqrt{2}\sqrt{(a^2+b^2)} - \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)}$$
$$= \frac{\sqrt{2}}{2}\sqrt{(a^2+b^2)} > |n+m+(m-n+1)i|.$$

If $|\mu| < \sqrt{2}$ or $\mu = 0$, ± 1, or $\pm i$ the same inequality holds unless $\mu = 0$. It can also be shown that for $x+yi$ in case 4, $|x+yi| \leqq |n+m+(m-n+1)i|$ and equality will hold for

$$x+yi = -n-m+(n-m-1)i,\ -n+m+1+(-n-m)i, \text{ or}$$
$$n-m-1+(n+m)i$$

all of which are vertices of the other three triangles. Therefore the representation is a "best" representation.

Notice that it was necessary to put the upper left hand corner point $-n+ni$ at point $-n+b-ni$ to take care of the cases where $n > 2m^2+2m+1$.

REPRESENTATION D. Since the components of $P = \bigcup_{\alpha\in R_2}(\delta R_1 \oplus \alpha)$ are disjoint and the cardinality of each $\delta R_1 \oplus \alpha = |\gamma|^2$, the cardinality of P is $|\gamma|^2|\delta|^2 = |\gamma\delta|^2$, i.e., just the proper size to be a representation of the CRS (mod $\gamma\delta$). If $\xi_1 = \delta\beta_1 + \alpha_1$ and $\xi_2 = \delta\beta_2 + \alpha_2$ are elements of P and if $\delta\beta_1 + \alpha_1 \equiv \delta\beta_2 + \alpha_2$ (mod $\gamma\delta$), then $\alpha_1 \equiv \alpha_2$ (mod δ) or $\alpha_1 = \alpha_2$ since both α_1 and α_2 are in R_2. Further, if $\gamma\delta | \delta(\beta_1 - \beta_2)$, then $\gamma | \beta_1 - \beta_2$; thus $\beta_1 = \beta_2$ since β_1 and β_2 are both in R_1. Thus distinct elements of P are incongruent modulo $\gamma\delta$ and therefore P is a representation of the CRS (mod $\gamma\delta$).

Reference

1. J. V. Uspensky and M. A. Heaslet, Elementary number theory, McGraw-Hill, New York, 1939.

A NOTE ON PRIMITIVE ROOTS

JOHN D. BAUM, Oberlin College

In teaching a one semester course in elementary number theory, the author has found that it is usually possible to finish the course by discussing quadratic reciprocity and a few of its consequences. The results which follow hang together in a mathematically esthetic fashion, utilize some of the results of quadratic reciprocity, and make some contribution to the theory of primitive roots. A cursory search of the literature reveals that at least one of these results (Theorem 1) appears not to be mentioned elsewhere, while others (Theorem 2) appear to be known. (Cf. [1] p. 127, Ex. 75 and 76, or [2], p. 122, Ex. 5.)

We shall deal with primes of the form $2q+1$, where q is an odd prime. We assume standard results on quadratic residues and primitive roots. An integer a, relatively prime to the prime p, belongs to the exponent $k>0$, modulo p, if $a^k \equiv 1 \pmod{p}$ and $a^n \not\equiv 1 \pmod{p}$ for $0<n<k$. A primitive root modulo p is a residue which belongs to the exponent $p-1$. It is a well-known result that if d is a divisor of $p-1$, then exactly $\phi(d)$ least positive residues belong to the exponent d, modulo p, where $\phi(x)$ is the Euler phi-function. There are thus $\phi(p-1)$ primitive roots, modulo p. A quadratic residue, modulo p, is an integer a such that $x^2 \equiv a \pmod{p}$ has solutions. The Legendre symbol, $(a|p)$, is defined for $(a, p)=1$ by the equations $(a|p)=1$ if a is a quadratic residue modulo p, and $(a|p)=-1$ if a is a quadratic nonresidue modulo p, i.e., $(a|p)=1$ if $x^2 \equiv a$ $\pmod{p}$ is solvable and $(a|p)=-1$ if $x^2 \equiv a \pmod{p}$ is not solvable. We extend the definition of the Legendre symbol to all integers by defining $(a|p)=0$ if p divides a, and we observe that $(a|p)=(b|p)$ if $a \equiv b \pmod{p}$. We note the following familiar results: a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. This result is known as Euler's criterion. From Euler's criterion it follows that $(-1|p)=(-1)^{(p-1)/2}$. If p and q are odd primes

$$(q\,|\,p) = (-1)^{(p-1)/2 \cdot (q-1)/2}(p\,|\,q);$$

this statement is one form of the law of quadratic reciprocity. Clearly no number is at one and the same time a quadratic residue and a primitive root modulo p, and there are exactly $(p-1)/2$ quadratic residues modulo p. In general $(ab|p)=(a|p)(b|p)$, and thus the product of a quadratic residue and a quadratic nonresidue is again a quadratic nonresidue.

We return now to primes of the form $p=2q+1$, where q is an odd prime, and consider first an example, $p=11$. We list the quadratic residues and primitive roots, indicating gaps in the two sequences by dashes, and the midpoint of the interval $[(p-1)/2, (p+1)/2]$ by a vertical stroke, "|".

Quadratic residues: 1, —, 3, 4, 5 | —, —, —, 9, — (mod 11).
Primitive roots: —, 2, —, —, — | 6, 7, 8, —, —, (mod 11).
We observe the following:

1. *With the exception of* $p-1$ ***every number*** a, $0<a<p$, *is either a quadratic residue or a primitive root modulo* p.

2. *If* a, $1<a<p-1$, *is a quadratic residue modulo* p, *then* $p-a$ *is a primitive root modulo* p, *and conversely.*

We prove these results for primes of the indicated form.

Proof of 1. The divisors of $p-1=2q$ are 1, 2, q and $2q$. $\phi(1)=1$, and the only number which belongs to the exponent 1 is 1 modulo p. $\phi(2)=1$ and only the number $p-1$ belongs to the exponent 2 modulo p. Thus every other least positive residue modulo p belongs either to $q=(p-1)/2$, i.e., is a quadratic residue by Euler's criterion, or to $2q=p-1$, i.e., is a primitive root.

Proof of 2. If a, $1<a<p-1$, is a quadratic residue modulo p, $(a|p)=1$. Then $(p-a|p)=(-a|p)=(-1|p)(a|p)=(-1|p)=(-1)^{(p-1)/2}=(-1)^q=-1$, since q is odd. Thus $p-a$ is a quadratic nonresidue; hence by 1 above a primitive root. The converse follows similarly.

We state our more interesting results in the following two theorems.

THEOREM 1. *If p and q are odd primes, $p=2q+1$, then if $q\equiv 1 \pmod 4$, $q+1$ is a primitive root modulo p, while if $q\equiv 3 \pmod 4$, q is a primitive root modulo p.*

Proof. In any case $p\equiv 3 \pmod 4$; thus if $q\equiv 1 \pmod 4$, $(q|p)=(p|q)=(2q+1|q)=(1|q)=1$. Thus q is a quadratic residue modulo p, and, by the preceding discussion, $p-q=2q+1-q=q+1$ is a primitive root. If $q\equiv 3 \pmod 4$, $(q|p)=-(p|q)=-(2q+1|q)=-(1|q)=-1$. Thus q is a quadratic nonresidue modulo p, hence a primitive root again by the preceding discussion. This completes the proof.

THEOREM 2. *If p and q are odd primes, $p=2q+1$, then $(-1)^{(q-1)/2}\cdot 2$ is a primitive root modulo p.*

Proof. If $q\equiv 1 \pmod 4$, $q+1$ is a primitive root by Theorem 1. Hence, since 4 is a quadratic residue, $4q+4\equiv 2\equiv(-1)^{(q-1)/2}\cdot 2 \pmod p$ is again a quadratic nonresidue, hence a primitive root modulo p. If $q\equiv 3 \pmod 4$, q is a primitive root by Theorem 1. Hence, since 4 is a quadratic residue, q a quadratic nonresidue, $4q\equiv -2\equiv(-1)^{(q-1)/2}\cdot 2 \pmod p$ is again a quadratic nonresidue, hence a primitive root modulo p. This completes the proof.

Since the search for primitive roots is generally quite tedious, Theorem 2 yields an expeditious method for finding primitive roots for a large class of primes.

References

1. Trygve Nagell, Introduction to number theory, Wiley, New York, 1951.
2. I. M. Vinogradov, Elements of number theory, Dover, New York, 1954.

THE DEFINITIONS OF THE EULER AND MÖBIUS FUNCTIONS

ECKFORD COHEN, University of Tennessee

1. It is customary to define the Euler totient function, $\phi(n)$, as the number of congruence classes $\{x\}$ with respect to the modulus n whose elements x are relatively prime to n, $(x, n)=1$. This definition may be viewed as additive in nature, since it is based upon the factor group J_n of the additive group of the integers modulo the subgroup generated by n. (In fact, $\phi(n)$ can be interpreted as the number of generators of the (cyclic) group J_n.) From this definition it follows easily that ϕ may be characterized multiplicatively as the function satisfying the relation

$$\sum_{d|n} \phi(d) = n, \tag{1}$$

for all $n\in J$, where J is the multiplicative semigroup of the positive integers.

It is possible to reverse this procedure; that is, we can start with (1) as the

We state our more interesting results in the following two theorems.

THEOREM 1. *If p and q are odd primes, $p=2q+1$, then if $q\equiv 1 \pmod 4$, $q+1$ is a primitive root modulo p, while if $q\equiv 3 \pmod 4$, q is a primitive root modulo p.*

Proof. In any case $p\equiv 3 \pmod 4$; thus if $q\equiv 1 \pmod 4$, $(q|p)=(p|q)=(2q+1|q)=(1|q)=1$. Thus q is a quadratic residue modulo p, and, by the preceding discussion, $p-q=2q+1-q=q+1$ is a primitive root. If $q\equiv 3 \pmod 4$, $(q|p)=-(p|q)=-(2q+1|q)=-(1|q)=-1$. Thus q is a quadratic nonresidue modulo p, hence a primitive root again by the preceding discussion. This completes the proof.

THEOREM 2. *If p and q are odd primes, $p=2q+1$, then $(-1)^{(q-1)/2}\cdot 2$ is a primitive root modulo p.*

Proof. If $q\equiv 1 \pmod 4$, $q+1$ is a primitive root by Theorem 1. Hence, since 4 is a quadratic residue, $4q+4\equiv 2\equiv(-1)^{(q-1)/2}\cdot 2 \pmod p$ is again a quadratic nonresidue, hence a primitive root modulo p. If $q\equiv 3 \pmod 4$, q is a primitive root by Theorem 1. Hence, since 4 is a quadratic residue, q a quadratic nonresidue, $4q\equiv -2\equiv(-1)^{(q-1)/2}\cdot 2 \pmod p$ is again a quadratic nonresidue, hence a primitive root modulo p. This completes the proof.

Since the search for primitive roots is generally quite tedious, Theorem 2 yields an expeditious method for finding primitive roots for a large class of primes.

References

1. Trygve Nagell, Introduction to number theory, Wiley, New York, 1951.
2. I. M. Vinogradov, Elements of number theory, Dover, New York, 1954.

THE DEFINITIONS OF THE EULER AND MÖBIUS FUNCTIONS

ECKFORD COHEN, University of Tennessee

1. It is customary to define the Euler totient function, $\phi(n)$, as the number of congruence classes $\{x\}$ with respect to the modulus n whose elements x are relatively prime to n, $(x, n)=1$. This definition may be viewed as additive in nature, since it is based upon the factor group J_n of the additive group of the integers modulo the subgroup generated by n. (In fact, $\phi(n)$ can be interpreted as the number of generators of the (cyclic) group J_n.) From this definition it follows easily that ϕ may be characterized multiplicatively as the function satisfying the relation

$$\sum_{d|n} \phi(d) = n, \tag{1}$$

for all $n\in J$, where J is the multiplicative semigroup of the positive integers.

It is possible to reverse this procedure; that is, we can start with (1) as the defining relation for the ϕ-function and deduce from this definition the additive interpretation by a very simple process. This fact is not widely appreciated and it is the aim of the present article to give an exposition of the details involved in the process. At the same time we shall deduce the additive meaning of the Möbius μ-function as the sum of the primitive nth roots of unity, proceeding from the multiplicative characterization of μ as the unique (multiplicative) function satisfying

$$\sum_{d|n} \mu(d) = \epsilon(n) = \begin{cases} 1 & (n = 1) \\ 0 & (n > 1). \end{cases} \tag{2}$$

In our discussion we replace the ϕ-function by the more general function ϕ_k, defined by

$$\sum_{d|n} \phi_k(d) = n^k \tag{3}$$

for all $k \in J$. Evidently, $\phi(n) = \phi_1(n)$. We shall characterize ϕ_k as the Jordan totient of order k, in terms of the equivalent formulation given by the author in [2]. That is, we show that $\phi_k(n)$ is the number of classes contained in the subset $T_k(n)$ of J_{n^k} defined to be the set of classes $\{x\}$ such that if $d|n$, then $d^k|x$ implies that $d=1$. Let $(x, n)_k = d^k$ if d is the largest divisor of n such that $d^k|x$; this may be stated simply: $\phi_k(n)$ is the number of $x \pmod{n^k}$ such that $(x, n)_k = 1$. (Evidently, if $x \equiv y \pmod{n^k}$, then $(x, n)_k = (y, n)_k$, so that the choice of residue system $x \pmod{n^k}$ is immaterial.)

The method of this note is based on an elementary use of trigonometric sums. If one is content to consider the ϕ-function alone, a purely arithmetical approach can be used (cf. the proof of Theorem 2 in [3]).

2. We consider functions $f(a, r)$, defined on the classes $\{a\}$ of J_r, $r \in J$, with values in the complex field. For each r, the class of all such functions forms a complex vector space S_r of dimension r with (orthonormal) basis

$$e(ax, r)/r, \qquad \{x\} \in J_r \qquad (e(a, r) = e^{2\pi i a/r});$$

hence $f(a, r)$ has the representation (cf. [4], Chp. 8, Sec. 5)

$$f(a, r) = \sum_{x \pmod{r}} \alpha_r(x) e(ax, r), \tag{4}$$

where

$$\alpha_r(x) = \frac{1}{r} \sum_{u \pmod{r}} f(u, r) e(-ux, r). \tag{5}$$

This representation can be established independently as follows. Placing $\eta(a, r) = 0$ or r according as $a \not\equiv 0 \pmod{r}$ or $a \equiv 0 \pmod{r}$, we have the familiar fact [5, p. 173] that,

$$\eta(a, r) = \sum_{x \pmod{r}} e(ax, r), \tag{6}$$

which results on summing a progression; substitution from (5) in connection with (6) is sufficient to verify (4).

3. We shall use the "Fourier" representation (4) of functions $f(a, r)$ of S_r with $r=n^k$. Let $\eta_k(a, n)=\eta(a, n^k)$; the defining relations (2) and (3) suggest consideration of the function $c_k(a, n)$ defined implicitly by

$$\sum_{d|n} c_k(a, d) = \eta_k(a, n); \tag{7}$$

in particular, noting that $\eta_k(0, n)=n^k$, $\eta_k(1, n)=\epsilon(n)$, we have

$$c_k(0, n) = \phi_k(n), \qquad c_k(1, n) = \mu(n). \tag{8}$$

Moreover, $c_k(a, n)\in S_{n^k}$; in fact, by Möbius inversion,

$$c_k(a, n) = \sum_{d|n} \eta_k(a, d)\mu\left(\frac{n}{d}\right) = \sum_{\substack{d|n \\ d^k|a}} d^k\mu\left(\frac{n}{d}\right). \tag{9}$$

We now determine the Fourier expansion of the function $c_k(a, n)$. Let

$$c_k(a, n) = \sum_{x \,(\mathrm{mod}\; n^k)} \alpha_k(x, n)e(ax, n^k), \tag{10}$$

so that, by (5),

$$\alpha_k(x, n) = \frac{1}{n^k} \sum_{u \,(\mathrm{mod}\; n^k)} c_k(u, n)e(-ux, n^k). \tag{11}$$

By (9) it follows that

$$\alpha_k(x, n) = \frac{1}{n^k} \sum_{u \,(\mathrm{mod}\; n^k)} \sum_{\substack{d|n \\ d^k|u}} d^k\mu\left(\frac{n}{d}\right)e(-ux, n^k).$$

Putting $u=d^kt$ and interchanging summations, we get

$$\begin{aligned} \alpha_k(x, n) &= \frac{1}{n^k} \sum_{d|n} d^k\mu\left(\frac{n}{d}\right) \sum_{t \,(\mathrm{mod}\; n^k/d^k)} e(-d^ktx, n^k) \\ &= \frac{1}{n^k} \sum_{d\delta=n} d^k\mu(\delta) \sum_{t \,(\mathrm{mod}\; \delta^k)} e(-tx, \delta^k). \end{aligned}$$

By (6) the inner sum is 0 unless $\delta^k | x$, in which case it has the value δ^k; therefore

$$\alpha_k(x, n) = \sum_{\substack{\delta|n \\ \delta^k|x}} \mu(\delta) = \sum_{\delta^k|(x,n^k)} \mu(\delta).$$

Let D^k denote the largest kth power divisor of x; then by (2),

$$\alpha_k(x, n) = \sum_{\delta|(D,n)} \mu(\delta) = \epsilon((D, n)) = \epsilon((x, n)_k). \tag{12}$$

Thus (10) becomes

$$c_k(a, n) = \sum_{\substack{x \pmod{n^k} \\ (x,n)_k=1}} e(ax, n^k). \tag{13}$$

This can also be proved implicitly, by comparing (7) and (6) with $r = n^k$.

By the first relation in (8) the case $a = 0$ in (13) gives the desired result,

$$\phi_k(n) = \sum_{\substack{x \pmod{n^k} \\ (x,n)_k=1}} 1; \tag{14}$$

the case $a = 1$, $k = 1$ in (13), by the second relation of (8), leads to

$$\mu(n) = \sum_{\substack{x \pmod{n} \\ (x,n)=1}} e(x, n). \tag{15}$$

The sum in (13) is the generalized Ramanujan sum introduced by the author in [1].

References

1. Eckford Cohen, An extension of Ramanujan's sum, Duke Math. J., 16 (1949) 85–90.
2. ———, Some totient functions, *Ibid.*, 23 (1956) 515–522.
3. ———, Quadratic congruences with an odd number of summands, Amer. Math. Monthly (to appear).
4. R. R. Stoll, Linear algebra and matrix theory, McGraw-Hill, New York, 1952.
5. I. M. Vinogradov, Elements of number theory. Translated from the 5th Russian edition. Dover, New York, 1954.

SUMS OF POWERS

MYRON TEPPER, University of Illinois

Let Q be a positive integer. From the identities

$$\sum_{i=1}^{n} i^Q = \sum_{i=0}^{n-1} (n - i)^Q, \tag{1}$$

$$n^Q + \sum_{i=1}^{n} (n - i)^Q = \sum_{i=1}^{n} [(n - i) + 1]^Q, \tag{2}$$

and

$$\sum_{i=1}^{n} (n - i)^Q = \sum_{i=1}^{n} i^Q - n^Q \tag{3}$$

two methods of finding sums of powers become evident:

Thus (10) becomes

$$c_k(a, n) = \sum_{\substack{x \pmod{n^k} \\ (x,n)_k=1}} e(ax, n^k). \tag{13}$$

This can also be proved implicitly, by comparing (7) and (6) with $r = n^k$.

By the first relation in (8) the case $a=0$ in (13) gives the desired result,

$$\phi_k(n) = \sum_{\substack{x \pmod{n^k} \\ (x,n)_k=1}} 1; \tag{14}$$

the case $a=1$, $k=1$ in (13), by the second relation of (8), leads to

$$\mu(n) = \sum_{\substack{x \pmod{n} \\ (x,n)=1}} e(x, n). \tag{15}$$

The sum in (13) is the generalized Ramanujan sum introduced by the author in [1].

References

1. Eckford Cohen, An extension of Ramanujan's sum, Duke Math. J., 16 (1949) 85–90.
2. ———, Some totient functions, *Ibid.*, 23 (1956) 515–522.
3. ———, Quadratic congruences with an odd number of summands, Amer. Math. Monthly (to appear).
4. R. R. Stoll, Linear algebra and matrix theory, McGraw-Hill, New York, 1952.
5. I. M. Vinogradov, Elements of number theory. Translated from the 5th Russian edition. Dover, New York, 1954.

SUMS OF POWERS

MYRON TEPPER, University of Illinois

Let Q be a positive integer. From the identities

$$\sum_{i=1}^{n} i^Q = \sum_{i=0}^{n-1} (n-i)^Q, \tag{1}$$

$$n^Q + \sum_{i=1}^{n} (n-i)^Q = \sum_{i=1}^{n} [(n-i)+1]^Q, \tag{2}$$

and

$$\sum_{i=1}^{n} (n-i)^Q = \sum_{i=1}^{n} i^Q - n^Q \tag{3}$$

two methods of finding sums of powers become evident:

I. Set $n^Q+\sum_{i=1}^{n}(n-i)^Q=\sum_{i=1}^{n}[(n-i)+1]^Q$ and solve for $\sum_{i=1}^{n}i^{Q-1}\{Q=1, 2, 3, \cdots\}$. We illustrate for $Q=2$ and $Q=3$.

A. Derivation of $\sum_{i=1}^{n}i=n(n+1)/2$.

By (2) with $Q=2$ we have

$$n^2+\sum_{i=1}^{n}(n-i)^2=\sum_{i=1}^{n}[(n-i)+1]^2=\sum_{i=1}^{n}(n-i)^2+\sum_{i=1}^{n}[2(n-i)+1].$$

Thus, $n^2=2\sum_{i=1}^{n}(n-i)+n$ and by (3), $n^2=2\sum_{i=1}^{n}i-2n+n$.

$$\therefore\ \sum_{i=1}^{n}i=\frac{n^2+n}{2}=\frac{n(n+1)}{2}.$$

B. Derivation of $\sum_{i=1}^{n}i^2=n(n+1)(2n+1)/6$.

By (2) with $Q=3$,

$$\begin{aligned}n^3+\sum_{i=1}^{n}(n-i)^3&=\sum_{i=1}^{n}[(n-i)+1]^3\\&=\sum_{i=1}^{n}[(n-i)^3+3(n-i)^2+3(n-i)+1],\end{aligned}$$

and by (3),

$$n^3=3\sum_{i=1}^{n}i^2-3n^2+3\sum_{i=1}^{n}i-3n+n=3\sum_{i=1}^{n}i^2-3n^2+\frac{3n(n+1)}{2}-2n,$$

$$2n^3=6\sum_{i=1}^{n}i^2-6n^2+3n^2+3n-4n.$$

$$\therefore\ \sum_{i=1}^{n}i^2=\frac{2n^3+3n^2+n}{6}=\frac{n(n+1)(2n+1)}{6}.$$

II. Solve

$$\sum_{i=1}^{n}i^Q=\sum_{i=1}^{n}[(n+1)-i]^Q \tag{4}$$

$$\sum_{i=1}^{n}i^Q=n^Q+\sum_{i=1}^{n}(n-i)^Q \tag{5}$$

for $\sum_{i=1}^{n}i^Q$ and $\sum_{i=1}^{n}i^{Q-1}\{Q=1, 3, 5, \cdots\}$. We illustrate for $Q=3$.

A. Derivation of

$$\sum_{i=1}^{n}i^3=\left[\frac{n(n+1)}{2}\right]^2 \quad\text{and}\quad \sum_{i=1}^{n}i^2=\frac{n(n+1)(2n+1)}{6}.$$

By (4) with $Q=3$,

$$\sum_{i=1}^{n}i^3=\sum_{i=1}^{n}[(n+1)-i]^3$$

$$= \sum_{i=1}^{n} [(n+1)^3 - 3(n+1)^2 i + 3(n+1)i^2 - i^3],$$

$$2\sum_{i=1}^{n} i^3 - 3(n+1)\sum_{i=1}^{n} i^2 = n(n+1)^3 - \frac{3n(n+1)^3}{2}$$

$$4\sum_{i=1}^{n} i^3 - 6(n+1)\sum_{i=1}^{n} i^2 = -n^4 - 3n^3 - 3n^2 - n \tag{6}$$

and by (5),

$$\sum_{i=1}^{n} i^3 = n^3 + \sum_{i=1}^{n}(n-i)^3 = n^3 + \sum_{i=1}^{n}(n^3 - 3n^2 i + 3ni^2 - i^3),$$

$$2\sum_{i=1}^{n} i^3 = n^3 + n^4 - \frac{3n^3(n+1)}{2} + 3n\sum_{i=1}^{n} i^2,$$

$$4\sum_{i=1}^{n} i^3 - 6n\sum_{i=1}^{n} i^2 = -n^4 - n^3. \tag{7}$$

Thus, subtracting (6) from (7), $6\sum_{i=1}^{n} i^2 = 2n^3 + 3n^2 + n$,

$$\sum_{i=1}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6} = \frac{n(n+1)(2n+1)}{6}$$

and from (7)

$$\sum_{i=1}^{n} i^3 = \frac{n(2n^3 + 3n^2 + n) - n^4 - n^3}{4} = \frac{n^4 + 2n^3 + n^2}{4} = \left[\frac{n(n+1)}{2}\right]^2.$$

CONCERNING ENVELOPES OF CERTAIN TRIGONOMETRIC POLYNOMIALS

RUSSELL A. WHITEMAN, Melpar, Inc., Falls Church, Va.

1. Introduction. In Goursat's, "A Course in Mathematical Analysis" [1] there is a well-known problem requiring the proof of the trigonometric identity

$$\sum_{p=0}^{n} \cos(a + pb) = \frac{\sin \dfrac{n+1}{2} b}{\sin \dfrac{b}{2}} \cos\left(a + \frac{nb}{2}\right). \tag{1}$$

This problem provides the mathematical basis of an electronic technique known as "Pulse Compression" used in modern radar systems [3]. By substituting the following quantities for a, b, and n,

$$= \sum_{i=1}^{n} [(n+1)^3 - 3(n+1)^2 i + 3(n+1)i^2 - i^3],$$

$$2\sum_{i=1}^{n} i^3 - 3(n+1)\sum_{i=1}^{n} i^2 = n(n+1)^3 - \frac{3n(n+1)^3}{2}$$

$$4\sum_{i=1}^{n} i^3 - 6(n+1)\sum_{i=1}^{n} i^2 = -n^4 - 3n^3 - 3n^2 - n \tag{6}$$

and by (5),

$$\sum_{i=1}^{n} i^3 = n^3 + \sum_{i=1}^{n} (n-i)^3 = n^3 + \sum_{i=1}^{n} (n^3 - 3n^2 i + 3ni^2 - i^3),$$

$$2\sum_{i=1}^{n} i^3 = n^3 + n^4 - \frac{3n^3(n+1)}{2} + 3n\sum_{i=1}^{n} i^2,$$

$$4\sum_{i=1}^{n} i^3 - 6n\sum_{i=1}^{n} i^2 = -n^4 - n^3. \tag{7}$$

Thus, subtracting (6) from (7), $6\sum_{i=1}^{n} i^2 = 2n^3 + 3n^2 + n$,

$$\sum_{i=1}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6} = \frac{n(n+1)(2n+1)}{6}$$

and from (7)

$$\sum_{i=1}^{n} i^3 = \frac{n(2n^3 + 3n^2 + n) - n^4 - n^3}{4} = \frac{n^4 + 2n^3 + n^2}{4} = \left[\frac{n(n+1)}{2}\right]^2.$$

CONCERNING ENVELOPES OF CERTAIN TRIGONOMETRIC POLYNOMIALS

RUSSELL A. WHITEMAN, Melpar, Inc., Falls Church, Va.

1. Introduction. In Goursat's, "A Course in Mathematical Analysis" [1] there is a well-known problem requiring the proof of the trigonometric identity

$$\sum_{p=0}^{n} \cos(a + pb) = \frac{\sin \frac{n+1}{2} b}{\sin \frac{b}{2}} \cos\left(a + \frac{nb}{2}\right). \tag{1}$$

This problem provides the mathematical basis of an electronic technique known as "Pulse Compression" used in modern radar systems [3]. By substituting the following quantities for a, b, and n,

$a=\omega t=2\pi ft$
$\omega=$smallest angular frequency in the sum of trigonometric terms
$f=$frequency corresponding to ω
$t=$time
$b=\Delta\omega\cdot t=2\pi\Delta f\cdot t$
$\Delta f=$frequency difference of the terms in the trigonometric polynomial
$n=N-1$
equation (1) becomes,

$$g(t)=\sum_{p=0}^{N-1}\cos(\omega+p\Delta\omega)t=\frac{\sin\frac{N\Delta\omega t}{2}}{\sin\frac{\Delta\omega t}{2}}\cos\left[\omega+\frac{(N-1)\Delta\omega}{2}\right]t. \tag{2}$$

The positive part of the envelope of (2) is denoted as $e(t)$ and is given by

$$e(t)=\left|\frac{\sin\frac{N\Delta\omega t}{2}}{\sin\frac{\Delta\omega t}{2}}\right|. \tag{3}$$

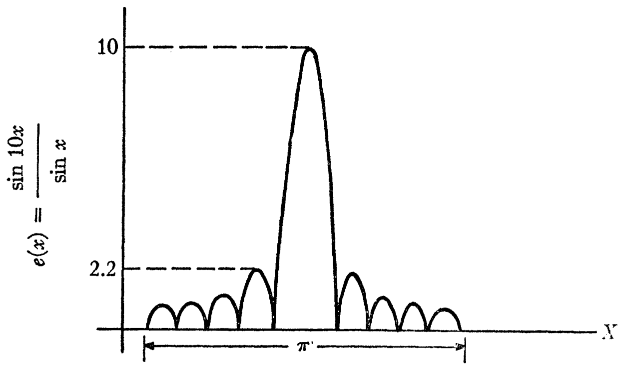


FIG. 1. Compressed-Pulse Envelope.

Equation (3) is depicted graphically in Figure 1, where $N=10$, $\Delta\omega t/2=x$, and $-\pi/2\leqq x\leqq\pi/2$. The graph in Figure 1 clearly shows why (3) is referred to as a "compressed pulse." The peaked pulse is identified with the radar target.

The purpose of this note is to present a method for determining the new envelope or "compressed pulse" when any one or more of the trigonometric terms on the left side of equation (1) are missing. A physical interpretation of this effect may be made by considering each cosine term in equation (2), and likewise in equation 1), as an alternating voltage generated by different circuits in the radar system. If one or more of these circuits fail to operate, then their voltages will not be generated and their corresponding cosine terms will be missing from the summation in equation (2). It will be shown that when certain terms of the trigonometric polynomial (1) are missing, the resultant envelope or new "compressed pulse" contains enlarged pulses which in turn may be interpreted as false radar targets.

2. Envelope with missing trigonometric terms. Let $\{p_i\}$, $i=1, 2, \cdots, K$ be a subsequence of $\{1, 2, \cdots, N-1\}$. Then $\{\omega+p_i\Delta\omega\}$ is a subsequence of the angular frequencies contained in (2). If the terms in (2) containing these frequencies are completely suppressed or removed, then the resultant envelope becomes the new "compressed pulse." To determine the equation for the envelope under these conditions, first express equation (2) with suppressed trigonometric terms as a family of curves in parametric form as follows,

$$F(g, t, s) = g - \frac{\sin \frac{N\Delta\omega t}{2}}{\sin \frac{\Delta\omega t}{2}} \cos \left[\omega + \frac{(N-1)\Delta\omega}{2} + s\right] t + \sum_{i=1}^{K} \cos (\omega + p_i\Delta\omega + s)t = 0, \tag{4}$$

where s is the parameter. The family of curves expressed by equation (4) are tangent to two curves defined as the envelope of (4). One of these curves lies above the abscissa and the other below. The curve above the abscissa will be the one of interest in this discussion. The coordinates of a point of the envelope [2] satisfy the simultaneous equations,

$$F(g, t, s) = 0, \qquad \frac{\partial F}{\partial s} = 0. \tag{5}$$

By eliminating the parameter s in the simultaneous equations (5), one obtains the equation of the new envelope $E(t)$ as,

$$E(t) = \pm \left\{ \left[\frac{\sin \frac{N\Delta\omega t}{2}}{\sin \frac{\Delta\omega t}{2}} \cos \frac{(N-1)\Delta\omega t}{2} - \sum_{i=1}^{K} \cos p_i\Delta\omega t \right]^2 + \left[\frac{\sin \frac{N\Delta\omega t}{2}}{\sin \frac{\Delta\omega t}{2}} \sin \frac{(N-1)\Delta\omega t}{2} - \sum_{i=1}^{K} \sin p_i\Delta\omega t \right]^2 \right\}^{1/2} \tag{6}$$

To illustrate (6) graphically when certain trigonometric terms of (2) are suppressed, consider the following numerical values, $N=10$, $p_i=3$, 4, 5, and 6, and let $-\pi/2 \leqq x \leqq \pi/2$ where $x=(\Delta\omega t)/2$. The graph of the positive part of (6) for these numerical values is depicted in Figure 2 and shows the changed envelope with a less defined "compressed pulse." The two enlarged pulses symmetrically

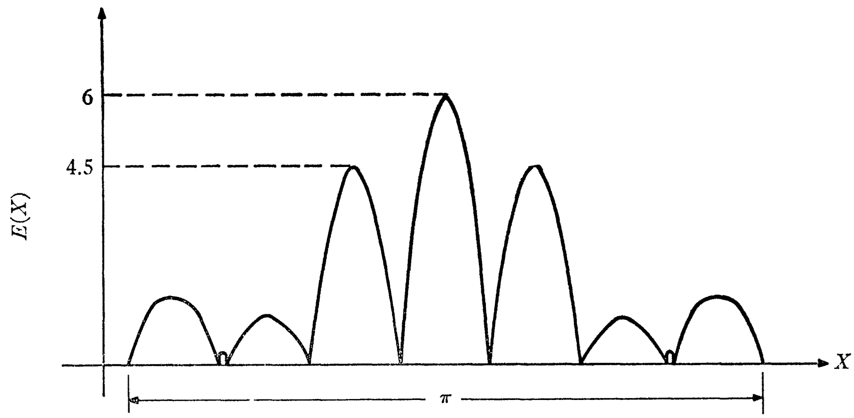


FIG. 2. "Compressed-Pulse" Envelope with Center Four Frequencies Suppressed where $N=10$, $p_i=3, 4, 5, 6$ in Equation (6).

spaced about the central pulse may be interpreted as false targets in a radar system.

This note is a by-product of a research program sponsored by Melpar, Inc., Falls Church, Virginia.

References

1. E. Goursat, A course in mathematical analysis, vol. 2, part 1, ch. 1, problem 5, p. 56, Dover, New York, 1959. Translated by E. R. Hedrick and O. Dunkel.
2. ———, *ibid.*, vol. 1, Ginn, New York, p. 426. Translated by E. R. Hedrick.
3. G. P. Ohman, Getting high range resolution with pulse compression radar, Electronics (Oct. 7, 1960) 53–57.

VARIOUS PROOFS OF PASCAL'S THEOREM

KAIDY TAN, Fukien Normal College, Foochow, China

This article is based on my lectures on geometrical methods which I have been accustomed to give to the students in the Fukien Normal College for the past several years, but it appears here with some improvements and additions. It has been proved by experience that it is of great value in training prospective geometry teachers to master various methods of geometry both advanced and elementary. I believe it can also stimulate the interest of some other readers. In this paper I treat only the special case of Pascal's Theorem by pure geometrical methods. Analytic methods are excluded since we can easily find these in any coordinate geometry text such as the works of Salmon, Loney, and so forth.

Pascal's Theorem is of great importance; it is a fundamental theorem in projective geometry (or modern synthetic geometry, sometimes called geometry of position). It was discovered by Blaise Pascal in 1639 when he was sixteen years old. We treat here only a special case of it.

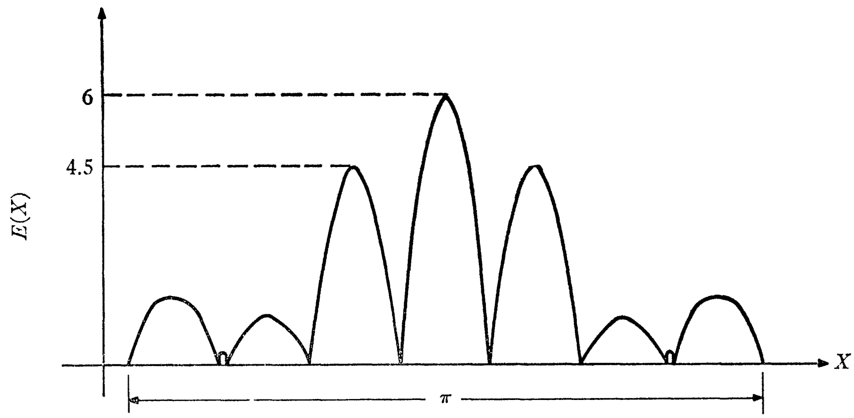


FIG. 2. "Compressed-Pulse" Envelope with Center Four Frequencies Suppressed where $N=10$, $p_i=3, 4, 5, 6$ in Equation (6).

spaced about the central pulse may be interpreted as false targets in a radar system.

This note is a by-product of a research program sponsored by Melpar, Inc., Falls Church, Virginia.

References

1. E. Goursat, A course in mathematical analysis, vol. 2, part 1, ch. 1, problem 5, p. 56, Dover, New York, 1959. Translated by E. R. Hedrick and O. Dunkel.

2. ———, *ibid.*, vol. 1, Ginn, New York, p. 426. Translated by E. R. Hedrick.

3. G. P. Ohman, Getting high range resolution with pulse compression radar, Electronics (Oct. 7, 1960) 53–57.

VARIOUS PROOFS OF PASCAL'S THEOREM

KAIDY TAN, Fukien Normal College, Foochow, China

This article is based on my lectures on geometrical methods which I have been accustomed to give to the students in the Fukien Normal College for the past several years, but it appears here with some improvements and additions. It has been proved by experience that it is of great value in training prospective geometry teachers to master various methods of geometry both advanced and elementary. I believe it can also stimulate the interest of some other readers. In this paper I treat only the special case of Pascal's Theorem by pure geometrical methods. Analytic methods are excluded since we can easily find these in any coordinate geometry text such as the works of Salmon, Loney, and so forth.

Pascal's Theorem is of great importance; it is a fundamental theorem in projective geometry (or modern synthetic geometry, sometimes called geometry of position). It was discovered by Blaise Pascal in 1639 when he was sixteen years old. We treat here only a special case of it.

Before we deal with the theorem, for briefness, we introduce some notations:

$A \cup B$: the line passing through A and B

$A \cup B \cup C$: three points A, B, and C are collinear

$AB \cap CD$: the meet (or intersection) of AB and CD

$AB \cap CD \cap EF$: the three lines AB, CD, and EF are concurrent

$\backsim$ is similar to (Note: This symbol is derived from the first letter of Latin *Similitudo*, some of the books misuse the symbols $\backsim$ or $\sim$ and confuse the two.)

$\backsim\!\!\!\!|$ is similar and similarly situated, i.e., homothetic relation,

$\doublebarwedge$ is in perspective with,

$\doteq$ is measured by,

⏢ quadrilateral,

$\measuredangle$ directed angle.

THEOREM. *The points of intersection of the opposite sides of a hexagon inscribed in a circle are collinear.*

Let $ABCDEF$ be any inscribed hexagon (the six vertices may be arranged in any order) and let $AB \cap DE = P$, $BC \cap EF = Q$, $CD \cap FA = R$. We are to prove that P, Q, and R are collinear ($P \cup Q \cup R$).

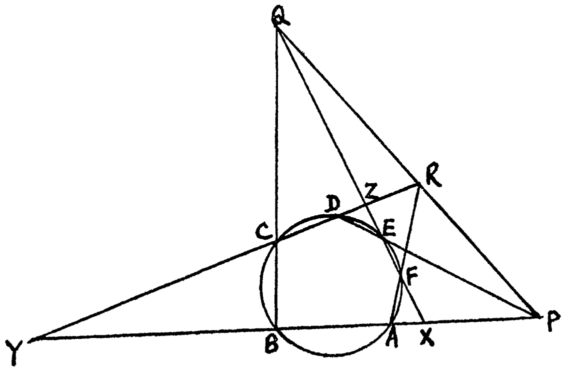


FIG. 1 (a).

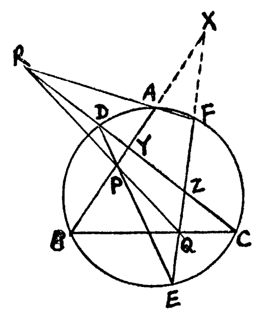


FIG. 1 (b).

Proof 1. Apply the theory of transversals (see Fig. 1). Let the three sides AB, CD, and EF (the first, the third, and the fifth side) form a triangle XYZ, and the three sides BC, DE, and FA (the second, the fourth, and the sixth side) be regarded as transversals respectively; we have

$$\frac{ZQ}{QX}\cdot\frac{XB}{BY}\cdot\frac{YC}{CZ} = -1, \quad \frac{XP}{PY}\cdot\frac{YD}{DZ}\cdot\frac{ZE}{EX} = -1, \quad \frac{YR}{RZ}\cdot\frac{ZF}{FX}\cdot\frac{XA}{AY} = -1$$

(by Menelaus Theorem).

Multiplying these three expressions side by side, we have

$$\frac{ZQ}{QX}\cdot\frac{XP}{PY}\cdot\frac{YR}{RZ}\cdot\frac{XB}{XE}\cdot\frac{XA}{XF}\cdot\frac{YC}{YA}\cdot\frac{YD}{YB}\cdot\frac{ZE}{ZC}\cdot\frac{ZF}{ZD} = -1. \tag{1}$$

But $XA \cdot XB = XE \cdot XF$, $YC \cdot YD = YA \cdot YB$, $ZE \cdot ZF = ZC \cdot ZD$. If we substitute in (1), we obtain

$$\frac{ZQ}{QX} \cdot \frac{XP}{PY} \cdot \frac{YR}{RZ} = -1. \qquad \therefore P \cup Q \cup R.$$

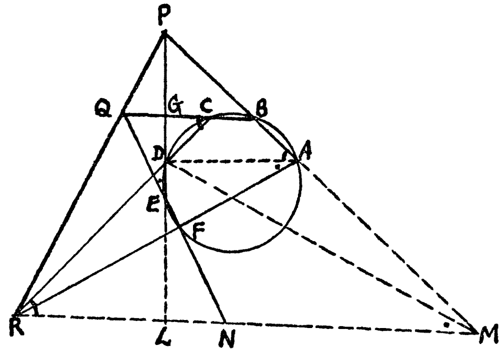


FIG. 2.

Proof 2. Apply theory of pencil of lines (see Fig. 2).

Draw $RM \| BC$ meeting DE, EF, AB at L, N, M respectively. Join DA, DM, and let $BC \cap DE = G$. Then $\angle BAD = \angle GCD = \angle DRM$. $\therefore D$, A, M, R are concyclic. Hence $\angle DMR = \angle DAR = \angle DEQ$. $\therefore D$, M, N, E are concyclic, so that $LE \cdot LD = LN \cdot LM$. Since

$$(2) \qquad \triangle GCD \sim \triangle LRD, \qquad \therefore \frac{DL}{LR} = \frac{GD}{GC} = \frac{GB}{GE}.$$

Again,

$$(3) \qquad \triangle GQE \sim \triangle LNE. \qquad \therefore \frac{GE}{QG} = \frac{LE}{LN} = \frac{LM}{LD}.$$

From (2) and (3), we have

$$\frac{GB}{GE} \cdot \frac{GE}{GQ} = \frac{DL}{LR} \cdot \frac{LM}{DL}. \qquad \therefore \frac{GB}{GQ} = \frac{LM}{LR}.$$

$\therefore (M \cup B) \cap (L \cup G) \cap (R \cup Q) \equiv P$; i.e., $P \cup Q \cup R$.

Proof 3. Apply the theorem on homothetic figures (see Fig. 3). Draw the circle ADR meeting PA, PE produced at G, H respectively. Join GH, GR, HR, GD, AD, and BE. Then, by the properties of the inscribed quadrilateral, we have $\angle GHD = \angle DAB = \angle DEB$. $\therefore HG \| EB$.

Again, $\angle RHD = \angle RAD = \angle QED$. $\therefore HR \| EQ$.
Again, $\angle RGA = \angle CDA = \angle QBP$. $\therefore QB \| RG$. $\therefore \triangle HGR \,\text{⌽}\, \triangle EBQ$.
Hence, $(G \cup B) \cap (H \cup E) \cap (R \cup Q) \equiv P$, $\therefore P \cup Q \cup R$.

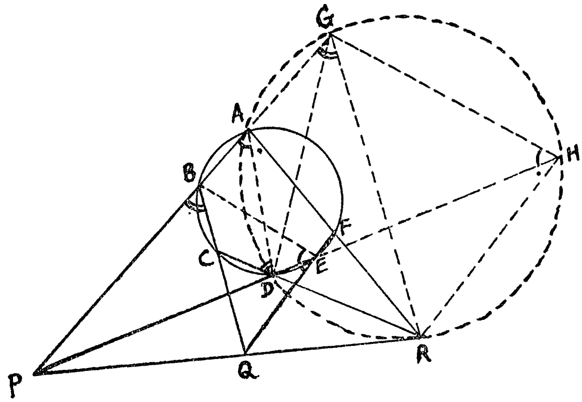


FIG. 3.

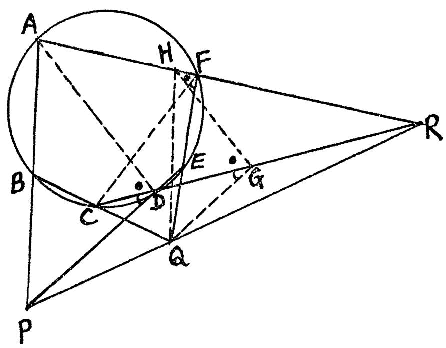


FIG. 4.

Proof 4. Alternate proof (see Fig. 4). Draw $QG \| PE$ meeting CR at G, and draw $GH \| AD$ meeting AR at H; join HQ and CF. Then $\angle QGC = \angle PDC = \angle CFG$; $\therefore C, F, G, G$ are concyclic. Again, $\angle HGC = \angle ADC = \angle AFC$. $\therefore H, F, G, C$ are concyclic. Hence, the five points C, F, H, G, Q are concyclic. $\therefore \angle QHG = \angle QCG = \angle BAD$. And since $AD \| HG$, $DP \| GQ$, $\therefore \angle ADP = \angle HGQ$. $\therefore \triangle ADP \sim \triangle HGQ$. Hence we have $(A \cup H) \cap (D \cup G) \cap (P \cup Q) \equiv R$; i.e., $P \cup Q \cup R$.

Proof 5. Apply the theorem on the inscribed angle of a circle (see Fig. 5). First, we may prove the following property:

$$\angle ARC = \angle APE + \angle EQC. \tag{4}$$

In Figure 5(a), we have

$$\angle APE \doteq \tfrac{1}{2}(\overset{\frown}{BCD} - \overset{\frown}{AFE}), \quad \angle EQC \doteq \tfrac{1}{2}(\overset{\frown}{FAB} - \overset{\frown}{EDC})$$

$$\angle ARC \doteq \tfrac{1}{2}(\overset{\frown}{ABC} - \overset{\frown}{FED}).$$

$$\begin{aligned}\therefore\ \angle APE + \angle EQC &\doteq \tfrac{1}{2}(\overset{\frown}{BCD} - \overset{\frown}{EDC}) + \tfrac{1}{2}(\overset{\frown}{FAB} - \overset{\frown}{AFE})\\ &\doteq \tfrac{1}{2}(\overset{\frown}{BC} - \overset{\frown}{DE}) + \tfrac{1}{2}(\overset{\frown}{AB} - \overset{\frown}{EF})\\ &\doteq \tfrac{1}{2}(\overset{\frown}{AB} + \overset{\frown}{BC}) - \tfrac{1}{2}(\overset{\frown}{DE} + \overset{\frown}{EF})\\ &\doteq \tfrac{1}{2}(\overset{\frown}{ABC} - \overset{\frown}{DEF}) \doteq \angle ARC.\end{aligned}$$

In Figure 5(b) we have

$$\angle APE \doteq \tfrac{1}{2}(AE + BD), \qquad \angle EQC \doteq \tfrac{1}{2}(\overset{\frown}{EC} + \overset{\frown}{BF}),$$

$$\angle ARC \doteq \tfrac{1}{2}(\overset{\frown}{AC} + \overset{\frown}{DF})$$

$$\therefore\ \angle APE + \angle EQC \doteq \tfrac{1}{2}(\overset{\frown}{AE} + \overset{\frown}{EC}) + \tfrac{1}{2}(\overset{\frown}{DB} + \overset{\frown}{BF}) \doteq \tfrac{1}{2}(\overset{\frown}{AC} + \overset{\frown}{DF}) \doteq \angle ARC.$$

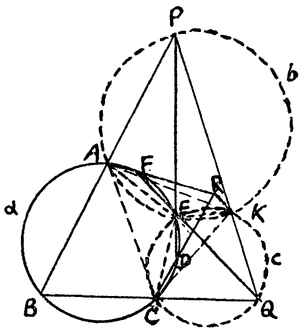


FIG. 5 (a).

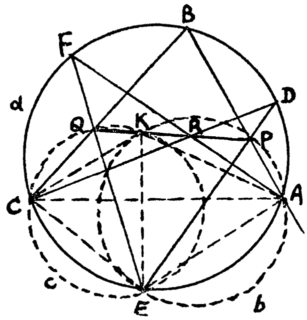


FIG. 5 (b).

Let the original circle ABC be $\odot a$; draw the circles APE and CQE and denote them by $\odot b$ and $\odot c$, and let K be the second point of intersection. Join KA, KC, KE, CE, EA, and AC. For brevity, we introduce directed angles. In both figures we have $\measuredangle PKE = \measuredangle BAE = \measuredangle BCE = 2$ rt. $\measuredangle$s $- \measuredangle EKQ$. $\therefore P \cup K \cup Q$.

Now in $\odot b$, we have $\measuredangle APE = \measuredangle AKE$. In $\odot c$, we have $\measuredangle EQC = \measuredangle EKC$. By adding these two expressions, and from (4), we get $\measuredangle ARC = \measuredangle AKC$. Hence A, R, K, C are concyclic, so that $\measuredangle RKA = \measuredangle RCA$. Now $\measuredangle RCA \equiv \measuredangle DCA = \measuredangle DEA \equiv \measuredangle PEA = \measuredangle PKA$. $\therefore \measuredangle RKA = \measuredangle PKA$. $\therefore K \cup R \cup P$. Hence the four points Q, K, P, R are collinear. $\therefore P \cup Q \cup R$.

Proof 6. Apply a theorem on a locus, (see Fig. 6). From Q draw the perpendiculars on BE, AB, DE, and denote their lengths as α, β, γ respectively. From R draw the perpendiculars on AD, AB, DE, and denote their lengths as α', β', γ' respectively. Now, because $\measuredangle EBC = \measuredangle EDC$, $\measuredangle CBA = \measuredangle CDA$, we have $\alpha/\gamma' = QB/RD = \beta/\alpha'$. Similarly, we have $QE/RA = \alpha/\beta' = \gamma/\alpha'$. $\therefore \alpha\alpha' = \beta\gamma' = \beta'\gamma$. $\therefore \beta/\gamma = \beta'/\gamma'$. But if a point moves so that the ratio of its distances from two intersection lines is constant, its locus is two intersecting lines passing through the meet of the two given lines. From this theorem we conclude that the three points P, Q, and R are collinear.

Proof 7. Apply a special theorem on an inscribed quadrilateral, (see Fig. 8).

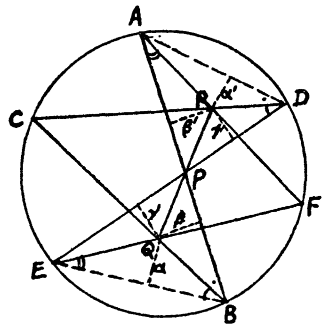


FIG. 6.

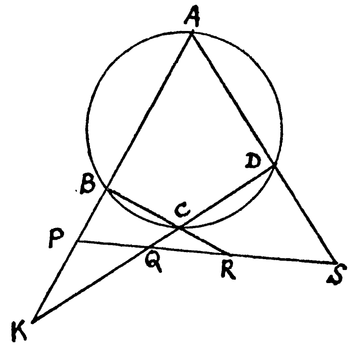


FIG. 7.

LEMMA. *A straight line intersects the four sides AB, BC, CD, and DA of an inscribed quadrilateral at P, R, Q, and S respectively. Then*

$$\frac{PR\cdot PS}{QR\cdot QS}=\frac{[P]}{[Q]}\,.$$

Here $[P]$ denotes the power of P with respect to the circumcircle; similarly for $[Q]$.

Proof of lemma: Let $(A\cup B)\cap(C\cup D)=K$. Now regarding the lines BCR, ADS as transversals of the $\triangle KPQ$, we have

$$\frac{RP}{QR}\cdot\frac{BK}{PB}\cdot\frac{CQ}{KC}=-1,\qquad \frac{SP}{QS}\cdot\frac{AK}{PA}\cdot\frac{DQ}{KD}=-1.$$

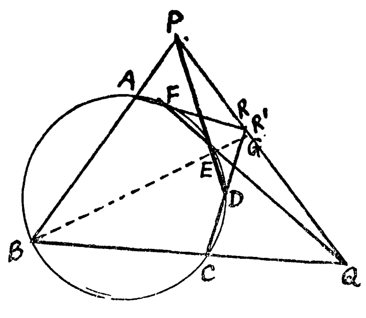


FIG. 8.

By multiplication, and making use of the property $AK\cdot BK=KC\cdot KD$, we have

$$\frac{RP\cdot SP}{QR\cdot QS}\cdot\frac{CQ\cdot DQ}{PB\cdot PA}=+1,\qquad \therefore\ \frac{PR\cdot PS}{QR\cdot QS}=\frac{[P]}{[Q]},\qquad \text{(see Fig. 7).}$$

Now we shall prove the Pascal Theorem as follows: Let $BC\cap EF=Q$, $AB\cap DE=P$, and CD, BE, AF intersect PQ at R', G, R respectively. Then in $\square\, ABEF$ and $\square\, BCDE$, by the lemma, we have

$$\frac{PG\cdot PR}{QG\cdot QR}=\frac{[P]}{[Q]}=\frac{PG\cdot PR'}{QG\cdot QR'}; \quad \text{hence} \quad \frac{PR}{QR}=\frac{PR'}{QR'}\cdot \quad \therefore R\equiv R',$$

i.e., the intersection of AF and CD is on the line PQ. $\therefore P\cup Q\cup R$.

Proof 8. Apply the theorem on the axis of similitude of three circles.

LEMMA. *If a circle cuts each of two given circles orthogonally, the line passing through each pair of intersecting points must pass through one of their homothetic centers.*

The proof is simple, so we omit it here.

Now we prove the theorem in the following manner: (Fig. 9).

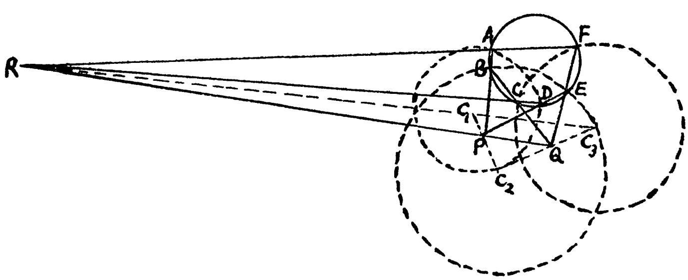


FIG. 9.

Through A, D draw $\odot c_1$ orthogonal to the given circle. (The center c_1 is the intersection point of the two tangents at A, D of the given circle.) And through B, E draw $\odot c_2$; through C, F draw $\odot c_3$, each orthogonal to the given circle. By the lemma we know that AB and DE both pass through one of the homothetic centers of the Ⓢc_1, c_2; hence their intersecting point P is one of the homothetic centers of the Ⓢc_1, c_2. Similarly, Q is one of the homothetic centers of the Ⓢc_2, c_3, and R is one of the homothetic centers of the Ⓢc_3, c_1.

As the positions of A, B, C, D, E, F vary, the three points P, Q, R are either the external centers of similitude, or two of them are the internal centers of similitude and the other is the external center of similitude of the three Ⓢc_1, c_2, c_3. By the theorem on the axis of similitude we know the three points P, Q, R are collinear. The details we omit here.

Proof 9. Apply the theory of involution, (see Fig. 10). Join AD and let the line EF cut AB, CD, BC, and AD at X, X', Q, and S respectively. Since $\triangle ABCD$ is inscribed in a circle, the line EF intersects the circle and the pairs of opposite sides of the quadrilateral in an involution. $\therefore \{EF, QS, XX'\}$ forms an involution range. But EF intersects $\triangle APDR$, the two diagonals, and the pairs of opposite sides in an involution also. Hence, if $RP\cap EF=Q'$, then $\{EF, SQ', XX'\}$ forms an involution range. $Q'\equiv Q$; i.e., $P\cup Q\cup R$.

Proof 10. Apply the theory of cross-ratio, (see Fig. 11).

Let $CD\cap BP=K$, $BC\cap DP=L$, and join AC, AD, EC, EB. Then $(KCDR)=A(KCDR)=A(BCDF)=E(BCDF)$. Again $E(BCDF)=E(BCLQ)=(BCLQ)$; i.e., $(KCDR)=(BCLQ)$. Now these two equicross ranges have a second corresponding point C in common. $\therefore KB\cap DL\cap RQ\equiv P$, i.e., $P\cup Q\cup R$.

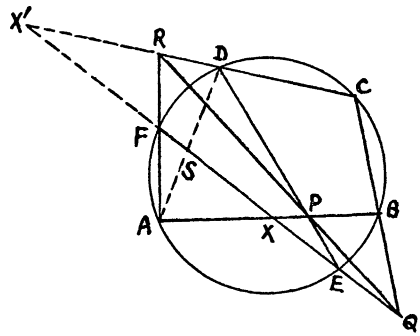


FIG. 10.

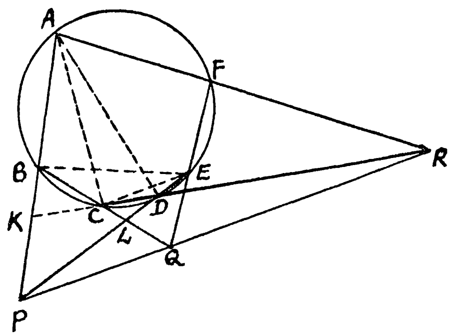


FIG. 11.

Proof 11. Alternate method, (see Fig. 12).

Draw the chords EA, EC, AD, CF, and join ER. Then $R(FQCE)=C(FBDE)$. Similarly, $R(APDE)=A(FBDE)$. But $A(FBDE)=C(FBDE)$. $\therefore R(APDE)=R(FQCE)$. Now these two equicross pencils have three rays ARF, DRC, RE in common. Therefore the other rays RP, RQ coincide. $\therefore P\cup Q\cup R$.

Proof 12. By the method of projection, (see Fig. 13).

Project RQ to infinity and the circumcircle into another circle; then the original figure 13(a) projects into figure 13(b). In the projection figure we have $bc\|ef$, $cd\|fa$. $\therefore \angle bcd=\angle efa$, $\therefore \overset{\frown}{bcd}=\overset{\frown}{efa}$; hence $ab\|de$; i.e., ab and de meet on the line of infinity. Hence in the original figure AB and DE meet on RQ, i.e., $P\cup Q\cup R$.

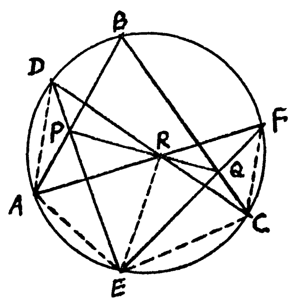


FIG. 12.

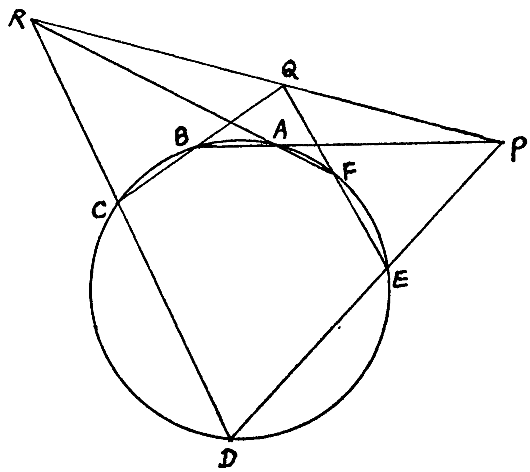


FIG. 13 (a).

Note. In this proof if the Pascal line PQR intersects the circumcircle the above method can not be applied. Now we give another method which can be applied in any case.

Proof 13. Alternate method. Project the point P to infinity and the circumcircle into another circle; then the original figure 13(a) projects into figure 13(c). In this figure, $ab\|de$. $\angle qfr=\angle abe=\angle bed=\angle qcr$. $\therefore q, r, c, f$ are concyclic; hence

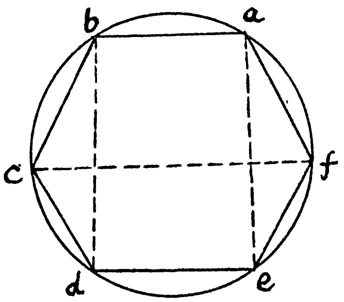


FIG. 13 (b).

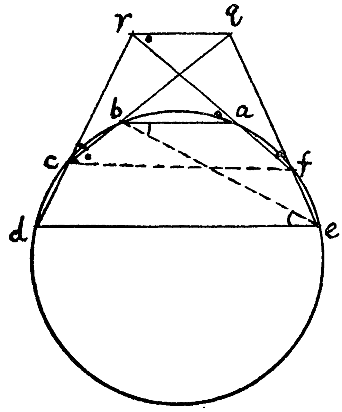


FIG. 13 (c).

$\angle qrf = \angle qcf = \angle bar$, $\therefore qr \| ab \| de$. Hence in the original figure QR, AB, and DE are concurrent, $\therefore P \cup Q \cup R$.

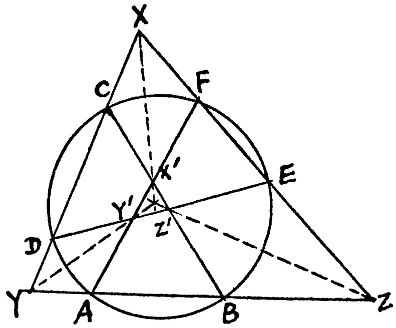


FIG. 14.

Proof 14. By the theory of perspective, (see Fig. 14).

Let AB, CD, EF form the $\triangle XYZ$ and AF, DE, BC the $\triangle X'Y'Z'$. Since A, B, C, D, E, F are concyclic, we have $XF \cdot XE = XC \cdot XD$, $YC \cdot YD = YA \cdot YB$, $ZA \cdot ZB = ZE \cdot ZF$.

$$\therefore \quad \frac{XF \cdot XE}{XC \cdot XD} \cdot \frac{YC \cdot YD}{YA \cdot YB} \cdot \frac{ZA \cdot ZB}{ZE \cdot ZF} = 1.$$

$\therefore$ by Lachlan [1] Section 177, $\triangle XYZ = \triangle X'Y'Z'$,
$\therefore$ $(YZ \cap Y'Z') \cup (ZX \cap Z'X') \cup (XY \cap X'Y')$,
i.e., $(AB \cap DE) \cup (EF \cap BC) \cup (CD \cap AF)$.

References

1. Robert Lachlan, An elementary treatise on modern pure geometry, London, Macmillan, 1893, pp. 177, 182, 281, 430.

2. John Casey, Sequel to elements of Euclid, 5th ed., Dublin, Hodges, Figgis & Company, 1888, Ch. 6, Th. 4.8.

3. A. Shively, Introduction to modern geometry, Chapman & Hall, London, 1939, pp. 9.6, 12.6.

4. Charles Godfrey and A. W. Siddons, Modern geometry, The University Press, Cambridge, England, 1928, Ch. 12.

5. R. A. Johnson, Modern geometry, Houghton Mifflin, Boston, New York, 1929, pp. 18, 19, 386.

THE MAXIMUM DIAMETER OF A CONVEX POLYHEDRON

E. JUCOVIČ AND J. W. MOON, Prešov Pedagogical Institute and University College, London

Let P_n denote a 3-dimensional convex polyhedron with n vertices. A sequence of edges of the form $\overline{ab}$, $\overline{bc}$, $\overline{cd}$, $\cdots$, $\overline{kl}$, $\overline{lm}$ is said to be a "path" from vertex a to vertex m. The "length" of a path is the number of edges it contains. If p and q are two vertices of P_n, the "distance" between p and q is defined as the length of the shortest path going from p to q. The "diameter" of P_n (in the graph theoretical sense (cf. [2], p. 12)), is the greatest distance between any two vertices of P_n. For example, according to this definition the diameter of a cube is 3 and that of a dodecahedron is 5. The main object in this note is to prove the following result.

THEOREM. *If d_n denotes the maximum diameter of all 3-dimensional convex polyhedra with n vertices, then* $d_n = [(n+1)/3]$.

Proof. According to a theorem of Balinski [1], the graph formed by the vertices and edges of any P_n is 3-connected, i.e., one can choose any two vertices of P_n and it is always possible to join any two of the remaining vertices by a path which doesn't pass through either of the two vertices originally chosen. This implies, by Menger's Theorem (cf. [2], p. 244), that for any two vertices p and q of P_n there are three paths going from p to q which have no vertices in common other than p and q. Suppose that p and q are two vertices of P_n whose distance apart equals the diameter d of P_n. Then each of the three paths going from p to q has length at least d, by definition, and hence each contains at least $d-1$ vertices other than p and q. As these vertices are all different it follows that $3(d-1)+2 \leqq n$, the total number of vertices of the polyhedron. Since d is an integer this implies that

$$d \leqq \left[\frac{n+1}{3}\right].$$

It is not difficult to construct a polyhedron for which equality holds here. The general idea of the construction when $n \equiv 2$ (modulo 3) should be clear from Figure 1. For the remaining cases one or both of the pyramidal caps at the ends may be removed. This suffices to complete the proof of the theorem.

This argument can easily be extended to treat the corresponding problem in k-dimensional space.

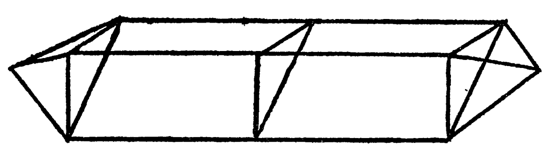


FIG. 1.

The "radius" of P_n (again in the graph theoretical sense) is the smallest integer r for which there exists a vertex p of P_n such that the distance from p to any other vertex of P_n is at most r. For example, the polyhedron in Figure 1 has radius 2. A natural question would be to ask what is the maximum radius r_n of all 3-dimensional convex polyhedra with n vertices? A simple example, illustrated in Figure 2 for $n=10$, shows that

$$r_n \geqq \left[\frac{n+4}{4}\right],$$

for $n \geqq 6$. We have not found any polyhedron P_n whose radius exceeds this quantity but we have been unable to prove that none such exists. The corresponding problem in higher dimensional space also remains unsolved.

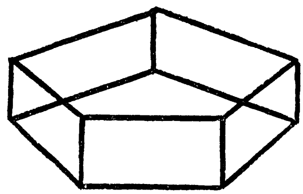


FIG. 2.

In closing we mention that if D_n denotes the maximum difference between the diameter and the radius of any polyhedron P_n, then it can be shown that

$$D_n = \left[\frac{n+1}{6}\right].$$

This follows upon observing that if d and r denote the diameter and radius of P_n, then $d \leqq 2r$, if d is even, and $d \leqq 2r-1$ if d is odd. The rest of the argument is straightforward and makes use of the above theorem. When $n \not\equiv 0, 1$ (modulo 6) the polyhedra represented in Figure 1 are examples for which $d-r=D_n$. With slight modifications the same is true for the remaining cases.

Acknowledgment of priority. The authors have just learned that the above theorem appears in "Longest Simple Paths in Polyhedral Graphs," J. London Math. Soc., 37 (1962) 152–160, by B. Grünbaum and T. S. Motzkin.

References

1. M. L. Balinski, On the graph structure of convex polyhedra in n-space, Pac. J. Math., 11 (1961) 431–434.

2. D. König, Theorie der endlichen und unendlichen Graphen, Leipzig, 1936. Reprinted Chelsea, New York, 1950.

A NOTE ON CIRCUMSCRIPTIBLE CYCLIC QUADRILATERALS

L. CARLITZ, Duke University

1. Let $ABCD$ denote a quadrilateral that is inscribed in one circle and circumscribed about another circle. Put $a=AB$, $b=BC$, $c=CD$, $d=DA$, $\alpha=\text{arc } AB$, $\beta=\text{arc } BC$, $\gamma=\text{arc } CD$ and $\delta=\text{arc } DA$. Let O denote the circumcenter and I the incenter of $ABCD$; let R denote the circumradius and r the inradius. Put $t=OI$, the distance between the circumcenter and the incenter.

The purpose of the present note is to find a formula for t analogous to the well-known formula of Euler for a triangle [1, p. 85]: $R^2-2Rr=d^2$. We shall show that

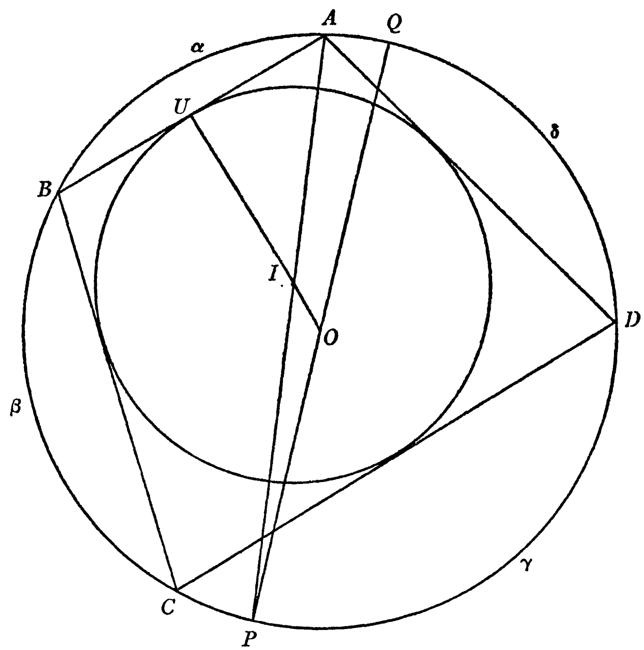
$$R^2 - t^2 = 2\lambda Rr, \tag{1}$$

where

$$\lambda = \frac{\cos \frac{1}{4}(\alpha + \gamma)}{\cos \frac{1}{4}(\alpha - \gamma)} \tag{2}$$

or equivalently

$$\lambda^2 = \frac{(ab + cd)(ad + bc)}{(a + c)^2(ac + bd)} \cdot \tag{3}$$



2. Let AI intersect the circumcircle in P, $P\neq A$, and let POQ be a diameter of the circle; also let U be the foot of the perpendicular from I on AB. Then it is easily verified that ΔBPQ is similar to ΔAIU, so that $PQ/AI=BP/IU$. Since $PQ=2R$, $IU=r$ and $AI\cdot IP=(R+t)(R-t)=R^2-t^2$, it follows that

$$2Rr = \frac{BP}{IP}(R^2 - t^2). \tag{4}$$

Since (see figure) $\measuredangle BAP=\frac{1}{4}(\beta+\gamma)$, $\measuredangle APB=\frac{1}{2}\alpha$, and $\measuredangle ABI=\frac{1}{4}(\gamma+\delta)$, it follows that $\measuredangle IBP=180°-\frac{1}{2}\alpha-\frac{1}{4}(\beta+\gamma)-\frac{1}{4}(\gamma+\delta)=\frac{1}{4}(\beta+\delta)=90°-\frac{1}{4}(\alpha+\gamma)$. Then $\measuredangle BIP=180°-\frac{1}{4}(\beta+\delta)-\frac{1}{2}\alpha=90°-\frac{1}{4}\alpha+\frac{1}{4}\gamma$, so that

$$\frac{BP}{IP}=\frac{\sin BIP}{\sin IBP}=\frac{\cos\frac{1}{4}(\alpha-\gamma)}{\cos\frac{1}{4}(\alpha+\gamma)}.$$

Thus (4) becomes

$$2Rr = (R^2 - t^2)\frac{\cos\frac{1}{4}(\alpha-\gamma)}{\cos\frac{1}{4}(\alpha+\gamma)},$$

which proves (2). Note that O, I, U, need not be colinear.

We remark that since $a+c=b+d$, $\sin\frac{1}{2}\alpha+\sin\frac{1}{2}\gamma=\sin\frac{1}{2}\beta+\sin\frac{1}{2}\delta$, so that $\sin\frac{1}{4}(\alpha+\gamma)\cos\frac{1}{4}(\alpha-\gamma)=\sin\frac{1}{4}(\beta+\delta)\cos\frac{1}{4}(\beta-\delta)$. It follows that

$$\lambda=\frac{\cos\frac{1}{4}(\alpha+\gamma)}{\cos\frac{1}{4}(\alpha-\gamma)}=\frac{\cos\frac{1}{4}(\beta+\delta)}{\cos\frac{1}{4}(\beta-\delta)}. \tag{5}$$

3. In order to prove (3) we take

$$a = 2R\sin\tfrac{1}{2}\alpha, \qquad b = 2R\sin\tfrac{1}{2}\beta, \qquad c = 2R\sin\tfrac{1}{2}\gamma, \qquad d = 2R\sin\tfrac{1}{2}\delta.$$

Then

$$\begin{aligned} ab + cd &= 4R^2(\sin\tfrac{1}{2}\alpha\sin\tfrac{1}{2}\beta+\sin\tfrac{1}{2}\gamma\sin\tfrac{1}{2}\delta) \\ &= 2R^2(\cos\tfrac{1}{2}(\alpha-\beta)+\cos\tfrac{1}{2}(\gamma-\delta)) \\ &= 4R^2(\sin\tfrac{1}{2}(\alpha+\gamma)\sin\tfrac{1}{2}(\alpha+\delta)). \end{aligned}$$

Similarly $ad+bc=4R^2\sin\frac{1}{2}(\alpha+\gamma)\sin\frac{1}{2}(\alpha+\beta)$, $ac+bd=4R^2\sin\frac{1}{2}(\alpha+\beta)\sin\frac{1}{2}(\alpha+\delta)$, while $a+c=4R\sin\frac{1}{4}(\alpha+\gamma)\cos\frac{1}{4}(\alpha-\gamma)$. Hence

$$\frac{(ab+cd)(ad+bc)}{(a+c)^2(ac+bd)}=\frac{\sin^2\frac{1}{2}(\alpha+\gamma)}{4\sin^2\frac{1}{4}(\alpha+\gamma)\cos^2\frac{1}{4}(\alpha-\gamma)}=\frac{\cos^2\frac{1}{4}(\alpha+\gamma)}{\cos^2\frac{1}{4}(\alpha-\gamma)}$$

and (3) follows at once.

4. It is of interest to recall that the quantities $ab+cd$, $ac+bd$, and $ad+bc$ have a simple geometric significance, namely they are products of pairs chosen from the three cyclic quadrilaterals obtained by permuting a, b, c, d. See for example [1, p. 128].

A more interesting observation is that (1) and (2) imply

$$R \geqq r\sqrt{2} \tag{6}$$

with equality if and only if $ABCD$ is a square. This is of course a special case of a more general theorem [2] but the present proof may be of some interest.

Clearly (6) is equivalent to $\lambda \geqq 1/\sqrt{2}$ with equality if and only if $ABCD$ is a square. Now since $\alpha+\beta+\gamma+\delta=360°$ we may assume (in view of (5)) that $\alpha+\gamma \leqq 180°$. Thus $\cos \frac{1}{4}(\alpha+\gamma) \geqq \cos 45° = 1/\sqrt{2}$. Therefore

$$\lambda = \frac{\cos \frac{1}{4}(\alpha + \gamma)}{\cos \frac{1}{4}(\alpha - \gamma)} \geqq \cos \frac{1}{4}(\alpha + \gamma) \geqq \frac{1}{\sqrt{2}} \cdot$$

Equality will occur if and only if $\alpha=\gamma=90°$, which requires $\beta=\delta=90°$. Then $a=c$ and $b=d$; since $a+c=b+d$ we get $a=b=c=d$.

Supported in part by NSF grant G16485.

References

1. N. A. Court, College geometry, Barnes and Noble, New York, 1952.
2. L. Fejes Tóth, Inequalities concerning polygons and polyhedra, Duke Math. J., 15(1948) 817–822.

CONSECUTIVE INTEGERS HAVING EQUAL SUMS OF SQUARES

J. S. VIGDER, Defence Research Board of Canada, Ottawa, Canada

The following investigation considers the problem of n consecutive integers and $m(<n)$ consecutive integers having equal sums of squares. The case where $m=1$ is discussed by Brother U. Alfred [1], who has established some necessary conditions for solutions to exist. The case where $m=n-1$ is posed as a problem in this MAGAZINE by Brother U. Alfred [2]; in this case formulas can be found giving all the solutions for any value of n.

The general problem can be stated thus: For given values of n and $m<n$, find integers x and z such that

$$\sum_{i=0}^{n-1} (x + i)^2 = \sum_{i=0}^{m-1} (z + i)^2.$$

Let $z=x+p$ and this reduces to

$$(1) \quad \begin{aligned} &(n - m)x^2 + \{n(n - 1) - m(m - 1) - 2mp\}x \\ &\quad + \tfrac{1}{6}\{n(n - 1)(2n - 1) - m(m - 1)(2m - 1)\} - m(m - 1)p - mp^2 = 0. \end{aligned}$$

To have rational solutions in x,

$$\begin{aligned} &\{n(n - 1) - m (m - 1) - 2mp\}^2 \\ &-4(n - m)[\tfrac{1}{6}\{n(n - 1)(2n - 1) - m(m - 1)(2m - 1)\} - m(m - 1)p - mp^2] = u^2 \end{aligned}$$

where u is an integer. Write $m=n-r$ and this reduces to

$$(2) \qquad 4np(n - r)(p - r) - \tfrac{1}{3}r^2(r - 1)(r + 1) = u^2.$$

of a more general theorem [2] but the present proof may be of some interest.

Clearly (6) is equivalent to $\lambda \geqq 1/\sqrt{2}$ with equality if and only if $ABCD$ is a square. Now since $\alpha+\beta+\gamma+\delta=360°$ we may assume (in view of (5)) that $\alpha+\gamma \leqq 180°$. Thus $\cos \frac{1}{4}(\alpha+\gamma) \geqq \cos 45° = 1/\sqrt{2}$. Therefore

$$\lambda = \frac{\cos \frac{1}{4}(\alpha + \gamma)}{\cos \frac{1}{4}(\alpha - \gamma)} \geqq \cos \frac{1}{4}(\alpha + \gamma) \geqq \frac{1}{\sqrt{2}} \cdot$$

Equality will occur if and only if $\alpha=\gamma=90°$, which requires $\beta=\delta=90°$. Then $a=c$ and $b=d$; since $a+c=b+d$ we get $a=b=c=d$.

Supported in part by NSF grant G16485.

References

1. N. A. Court, College geometry, Barnes and Noble, New York, 1952.
2. L. Fejes Tóth, Inequalities concerning polygons and polyhedra, Duke Math. J., 15(1948) 817–822.

CONSECUTIVE INTEGERS HAVING EQUAL SUMS OF SQUARES

J. S. VIGDER, Defence Research Board of Canada, Ottawa, Canada

The following investigation considers the problem of n consecutive integers and $m(<n)$ consecutive integers having equal sums of squares. The case where $m=1$ is discussed by Brother U. Alfred [1], who has established some necessary conditions for solutions to exist. The case where $m=n-1$ is posed as a problem in this MAGAZINE by Brother U. Alfred [2]; in this case formulas can be found giving all the solutions for any value of n.

The general problem can be stated thus: For given values of n and $m<n$, find integers x and z such that

$$\sum_{i=0}^{n-1} (x+i)^2 = \sum_{i=0}^{m-1} (z+i)^2.$$

Let $z=x+p$ and this reduces to

$$\begin{aligned}(n-m)x^2 &+ \{n(n-1) - m(m-1) - 2mp\}x \\ &+ \tfrac{1}{6}\{n(n-1)(2n-1) - m(m-1)(2m-1)\} - m(m-1)p - mp^2 = 0.\end{aligned} \tag{1}$$

To have rational solutions in x,

$$\begin{aligned}&\{n(n-1) - m(m-1) - 2mp\}^2 \\ &-4(n-m)[\tfrac{1}{6}\{n(n-1)(2n-1) - m(m-1)(2m-1)\} - m(m-1)p - mp^2] = u^2\end{aligned}$$

where u is an integer. Write $m=n-r$ and this reduces to

$$4np(n-r)(p-r) - \tfrac{1}{3}r^2(r-1)(r+1) = u^2. \tag{2}$$

When integers p, u satisfying the above are found, we can write

$$(3) \qquad x = \frac{-\{n(n-1) - m(m-1) - 2mp\} \pm u}{2r}, \qquad z = x + p.$$

Note that while the existence of integers p, u satisfying (2) is a necessary condition for integers x, z to exist, it is not a sufficient condition, since $2r$ occurs in the denominator of x as given by (3).

For any given n, m we can solve the problem by determining if integers p, u exist which satisfy (2) and yield integral values of x. Ultimately all cases reduce to equations of the form.

$$(4) \qquad as^2 - bt^2 = c,$$

where a, b, c are positive integers and the equation must be solved in integers for s and t, with p a linear function of s and u a multiple of t. We shall assume that all common factors of a, b, c are eliminated; if a and b are both square numbers, (4) will have at most a finite number of solutions, in all other cases (4) will have either no solutions or an infinite number [**3**]. When (4) has an infinite number of solutions they are all determined by taking a finite number of solutions and extending this finite set by means of a recursion formula [**3**].

Example. $n=11$, $m=5$, $\therefore r=6$.

From (2): $220p(p-6)-420=u^2$. This reduces to: $55s^2-t^2=6$, where $p-3=10s$ and $u=20t$.

This equation has an infinite number of solutions in (s, t) of which the first four in positive integers are (1, 7), (5, 37), (173, 1283), (889, 6593). If we let $s_1=1$, $t_1=7$ and $s_2=173$, $t_2=1283$, then the recursion formulas

$$s_{i+1} = 178s_i - s_{i-1}, \qquad t_{i+1} = 178t_i - t_{i-1}$$

will generate an infinite set of solutions. If we let $s_1=5$, $t_1=37$, and $s_2=889$, $t_2=6593$, the same recursion formulas will generate a second set of solutions. These two sets, together with the solutions obtained by introducing negative signs, constitute all the solutions (s, t); to show that there are no other solutions it is only necessary to verify that for $1<s<173$ there is no solution other than $s=5$, $t=37$. After having found the appropriate values of p and u we obtain x and z from (3). Thus for $s=1$, $t=7$, we have $p=13$, $u=140$. From (3) we get

$$x = \frac{-\{11(10) - 5(4) - 2(5)(13)\} \pm 140}{12} = \frac{40 \pm 140}{12} = 15$$

(only the positive sign gives an integral value of x here), $z=15+13=28$, so that $15^2+\cdots+25^2=28^2+\cdots+32^2$. In this particular case, for every solution (s, t) we get one solution in integers of (x, z).

From the recursion formulas for s and t we can obtain recursion formulas giving x and z. Substituting $p=10s+3$, $u=20t$ directly in (3) we get in this example

$$x = \frac{25s \pm 5t}{3} - 5, \qquad z = x + 10s + 3.$$

$s_1=1$, $t_1=7$ yields the solution $x_1=15$, $z_1=28$; $s_2=173$, $t_2=1283$ yields the solution $x_2=3575$, $z_2=5308$. Now

$$\begin{aligned} x_{i+1} &= \frac{25s_{i+1}+5t_{i+1}}{3} - 5 \quad \text{(where the positive sign, only, gives integral values of } x \text{ here)} \\ &= \frac{25(178s_i - s_{i-1}) + 5(178t_i - t_{i-1})}{3} - 5 \\ &= 178\left\{\frac{25s_i+5t_i}{3} - 5\right\} - \left\{\frac{25s_{i-1}+5t_{i-1}}{3} - 5\right\} + 880 \\ &= 178x_i - x_{i-1} + 880. \end{aligned}$$

Similarly $z_{i+1}=178z_i-z_{i-1}+352$.

Taking the solutions given by $s_1=5$, $t_1=37$ and $s_2=889$, $t_2=6593$, the same recursion formulas in (x, z) would yield a second set of solutions; only the negative sign in the numerator of (3) will yield integral values of x. In this particular case the second set will not really be different solutions; they will be equivalent to the first set with the signs of the n numbers reversed.

Number of solutions. In those cases where a and b in equation (4) are perfect squares, (4) can have at most a finite number of solutions (s, t) and hence there can, at most, be a finite number of solutions for (x, z). If (4) has no solutions there are, of course, no solutions for (x, z). If a and b are not both perfect squares and one solution (s, t) of (4) exists, there are a finite number of infinite sets of solutions and each of these infinite sets can be generated by a linear recursion formula [3]. The recursion formula for solutions of $as^2-bt^2=c$, when such exist, is in fact the same recursion formula which generates solutions of the Pell Equation $s^2-abt^2=1$. When a solution (s, t) will yield a solution (x, z) the numerator in (3) can be expressed as a linear function of s and t which is a multiple of $2r$. Now if a linear function of s_i and t_i is divisible by a number N for one i, it will be divisible by N for an infinite set of i. Furthermore, this set of (s_i, t_i) will occur at regular intervals in the infinite sets of solutions generated by the recursion formula. Hence the set of (s_i, t_i) which yield solutions (x, z) can themselves be generated by recursion formulas, and the solutions (x, z) are also generated by recursion formulas. Thus when a and b of (4) are not both perfect squares and one solution (x, z) exists, there will be an infinite number of solutions which can be generated by recursion formulas operating upon a finite number of solutions. The method of obtaining these solutions and recursion formulas is illustrated in the example above.

m = 1. The case where $m=1$ is discussed at some length in [1], where a number of necessary conditions are established for solutions to exist. For $n \leqq 500$, solutions were found in 52 cases, shown not to exist in 443 cases and 5 values of n were left unresolved, viz. 107, 193, 227, 275, 457.

When $m=1$, $n=r+1$, and (2) becomes

$$4(r+1)p(p-r) - \tfrac{1}{3}r^2(r-1)(r+1) = u^2 \tag{5}$$

and (3) reduces to

$$(6) \qquad x = \frac{-r(r+1) + 2p \pm u}{2r}, \qquad z = x + p.$$

When $n = r+1$ is not a multiple of 3, (5) can be reduced to

$$4p(p - r) - \tfrac{1}{3}r^2(r - 1) = \alpha u'^2,$$

where $n = \alpha\beta^2$, β^2 being the largest square that divides into n, and $u = \alpha\beta u'$. This can be written in the form

$$(7) \qquad (2p - r)^2 - \tfrac{1}{3}r^2(r + 2) = \alpha u'^2.$$

If no square greater than 1 divides into n, (7) becomes

$$(7') \qquad (2p - r)^2 - \tfrac{1}{3}r^2(r + 2) = (r + 1)u'^2, \qquad u = (r + 1)u'.$$

When $n = r+1 = \beta^2$, (7) becomes $(2p-r)^2 - u'^2 = \frac{1}{3}r^2(r+2)$ and there are thus, at most, a finite number of solutions.

When $n = 3k^2 - 1$, there will always be an infinite number of solutions. In this case (7′) becomes

$$(2p - r)^2 - \tfrac{1}{3}r^2(3k^2) = (r + 1)u'^2, \qquad u = (r + 1)u'.$$

We deal with (7′) rather than (7) since we are going to show how to find some of the solutions, not necessarily all of them. The above equation can be written

$$(8) \qquad (2p - r)^2 - (r + 1)u'^2 = r^2k^2, \qquad u = (r + 1)u'.$$

Consider the Pell Equation

$$(9) \qquad s^2 - nt^2 = 1$$

which has an infinite number of solutions, since n is not a square. For every (s_i, t_i) which is a solution of (9), $2p - r = rks_i$, $u' = rkt_i$ is a solution of (8). Since k and s_i are odd if r is odd, we have $p = \frac{1}{2}r(ks_i + 1)$, $u = r(r+1)kt_i$ as integral solutions of (8). From (6),

$$x_i = \frac{-r(r+1) + rks_i + r \pm r(r+1)kt_i}{2r} = \tfrac{1}{2}k\{s_i \pm (r+1)t_i\} - \tfrac{1}{2}r$$

$$z_i = \tfrac{1}{2}k(r+1)(s_i \pm t_i).$$

i.e.,

$$(10) \qquad x_i = \tfrac{1}{2}\sqrt{(\tfrac{1}{3}(n+1))}(s_i \pm nt_i) - \tfrac{1}{2}(n-1), \quad z_i = \tfrac{1}{2}n\sqrt{(\tfrac{1}{3}(n+1))}(s_i \pm t_i).$$

If (s_1, t_1) is the smallest solution in positive integers of the Pell Equation (9), we have

$$s_{i+1} = 2s_1s_i - s_{i-1}, \qquad t_{i+1} = 2s_1t_i - t_{i-1}$$

$$x_{i+1} = \tfrac{1}{2}\sqrt{(\tfrac{1}{3}(n+1))}\cdot(2s_1s_i - s_{i-1} + 2ns_1t_i - nt_{i-1}) - \tfrac{1}{2}(n-1)$$

$$z_{i+1} = \tfrac{1}{2}n\sqrt{(\tfrac{1}{3}(n+1))}\cdot(2s_1s_i - s_{i-1} + 2s_1t_i - t_{i-1}).$$

Thus

$$x_{i+1} = 2s_1x_i - x_{i-1} + (s_1 - 1)(n - 1), \qquad z_{i+1} = 2s_1z_i - z_{i-1}. \tag{11}$$

If we take

$$x_0 = \tfrac{1}{2}(\sqrt{(\tfrac{1}{3}(n + 1))} - n + 1), \qquad z_0 = \tfrac{1}{2}n\sqrt{(\tfrac{1}{3}(n + 1))} \tag{12}$$

which are the solutions corresponding to $s_0 = 1$, $t_0 = 0$, and (x_1, z_1) as the solutions corresponding to (s_1, t_1), we have recursion formulas which give an infinite number of solutions, but not necessarily all of them.

Example: $n = 11 = 3(2^2) - 1$.

The Pell Equation (9) is

$$s^2 - 11t^2 = 1; \qquad s_1 = 10, \qquad t_1 = 3.$$

From (12): $\quad x_0 = -4, \quad z_0 = 11;$

From (10): $\quad x_1 = 38, \quad z_1 = 143;$

From (11): $\quad x_{i+1} = 20x_i - x_{i-1} + 90, \quad z_{i+1} = 20z_i - z_{i-1}.$

If we reverse the recursion formulas to give solutions in negative numbers (or use the negative sign in the numerator of x), we arrive at the equivalent of the following solutions:

$$x_0 = -6, \qquad z_0 = 11, \qquad x_1 = 18, \qquad z_1 = 28$$

and the same recursion formulas as above.

To obtain all the solutions for $n = 11$ it is necessary to solve completely the equation $s^2 - 11t^2 = 100$, where $p = s + 5$ and $u = 22t$. All the solutions are given by the recursion formulas

$$s_{i+1} = 20s_i - s_{i-1}, \qquad t_{i+1} = 20t_i - t_{i-1}$$

where (s_0, t_0) and (s_1, t_1) are taken in turn to be $(54, -16)$ and $(12, 2)$; $(12, -2)$ and $(54, 16)$; $(10, 0)$ and $(100, 30)$. However, on substituting the appropriate values of p and u in (6), it can be seen that in this particular case no solutions will be forthcoming other than those already obtained.

It so happens that one of the unresolved numbers in [1] is of the type $3k^2 - 1$, $107 = 3(6^2) - 1$. For the Pell Equation $s^2 - 107t^2 = 1$ we have $s_1 = 962$, $t_1 = 93$. Making the appropriate substitutions in (12) and (10), we get

$$x_0 = -50, \quad z_0 = 321; \qquad x_1 = 32686, \quad z_1 = 338655$$

and from (11) we can get the recursion formulas. Taking the negative sign in the numerator of x, we can get the equivalent of the following

$$x_0 = -56, \quad z_0 = 321; \qquad x_1 = 26914, \quad z_1 = 278949$$

with the same recursion formulas as above. We have no assurance, however, that this gives all the solutions.

Example: $n=24$. In this case, since 24 is a multiple of 3, we cannot use (7), and from (5) we get

$$4(24)p(p-23)-\tfrac{1}{3}(23^2)(22)(24)=u^2$$

$$6p(p-23)-11(23^2)=u'^2, \qquad u=4u'$$

$$3(2p-23)^2-2u'^2=115^2. \tag{13}$$

Now if s_i, t_i is a solution of

$$3s^2-2t^2=1, \tag{14}$$

then $p_i=\frac{1}{2}(115s_i+23)$, $u_i'=115t_i$ is a solution of (13). All the solutions of (14) are given by

$$s_{i+1}=10s_i-s_{i-1}, \qquad t_{i+1}=10t_i-t_{i-1}$$

$$s_1=1, \quad t_1=1; \qquad s_2=9, \quad t_2=11.$$

Corresponding to (s_1, t_1) we have $p_1=69$, $u_1=4u_1'=460$ and, from (6), $x_1=1$, $z_1=70$ and to (s_2, t_2), $x_2=121$, $z_2=650$. Following the method used in the earlier examples we obtain the recursion formulas:

$$x_{i+1}=10x_i-x_{i-1}+92, \qquad z_{i+1}=10z_i-z_{i-1}. \tag{15}$$

By completely solving $3s^2-2t^2=115^2$ we can show that all solutions in positive integers when $n=24$ are given by recursion formulas (15) when (x_1, z_1) and (x_2, z_2) are taken in turn as:

(1, 70) and (121, 650)	(25, 182) and (353, 1786)
(9, 106) and (197, 1022)	(44, 274) and (540, 2702)
(20, 158) and (304, 1546)	(76, 430) and (856, 4250)

Two of the other unresolved values of n in [1] can be shown to yield no solutions. For $n=275$, (7) becomes

$$(2p-274)^2-\tfrac{1}{3}(274)^2(276)=11u'^2, \qquad u=55u'.$$

Thus we must solve the equation

$$s^2-11t^2=2^2(23)(137)^2, \qquad p=s+137, \qquad u=110t.$$

If s and t are both odd we have $s^2-11t^2\equiv 2 \pmod 4$ and hence s and t must both be even. Putting $s=2s'$, $t=2t'$, we get $s'^2-11t'^2=23(137)^2$, and $23(137)^2 \equiv 3 \pmod 4$. Since one of s, t is odd and the other even we have $s'^2-11t'^2 \equiv 1 \pmod 4$ and hence no solution exists.

For $n=227$, (7′) becomes

$$(2p-226)^2-\tfrac{1}{3}(226)^2(228)=227u'^2, \qquad u=227u'$$

and we must solve

$$s^2-227t^2=2^2(19)(113)^2, \qquad u=454t, \qquad p=s+113.$$

Just as in the previous case we can show that both sides of this equation cannot be congruent modulo 4, and hence no solution exists.

For $n=193$, (7′) becomes $(2p-192)^2-\frac{1}{3}(192)^2(194)=193u'^2$, $u=193u'$ and we must solve

$$s^2 - 193t^2 = 2^{11}(3)(97); \qquad p = s + 96, \quad u = 386t.$$

This equation has the solution $t=56$, $s=1096$ and hence has an infinite number of solutions [3]. Corresponding to the above solution we have $x=-34$, $z=1158$ so that $(-34)^2+\cdots+(158)^2=1158^2$. Since there are an infinite number of solutions for (x, z) there will be some with $|x|>193$ and hence solutions in positive integers exist.

For the final unresolved case in [1], $n=457$, (7′) becomes

$$(2p - 456)^2 - \tfrac{1}{3}(456)^2(458) = 457u'^2, \qquad u = 457u'$$

so that we must solve

$$s^2 - 457t^2 = 2^5(3)(19)^2(229); \qquad p = s + 228, \quad u = 914t.$$

This equation has an infinite number of solutions, e.g., $t=266$, $s=6346$, but it has not been determined whether any of them yield integral values of x.

The $n+m$ integers are consecutive, that is $p=n$. In [2] it is shown that when $m = n - 1$ there will always be one solution in positive integers, viz. $x=(n-1)(2n-1)$, $z=2n^2-2n+1$.

For $p=n$, (2) reduces to $4n^2(n-r)^2-\frac{1}{3}r^2(r-1)(r+1)=u^2$ or

$$n^2(n - r)^2 - r^2(r - 1)(r + 1)/12 = u'^2, \qquad u = 2u'. \tag{16}$$

We can put

$$n(n - r) = \tfrac{1}{2}(A + B), \quad u' = \tfrac{1}{2}(A - B), \text{ where } AB = r^2(r - 1)(r + 1)/12 \tag{17}$$

and we must seek values of A and B that yield integral values of n, r, and u. If we let $A=\frac{1}{2}r(r-1)$ and $B=\frac{1}{6}r(r+1)$, we get from (17) that

$$n(n - r) = \tfrac{1}{6}r(2r - 1) \quad \text{and} \quad u = \tfrac{1}{3}r(r - 2).$$

From the first of these equations, we have

$$n^2 - nr + \tfrac{1}{4}r^2 = \tfrac{1}{6}r(2r - 1) + \tfrac{1}{4}r^2,\ (n - \tfrac{1}{2}r)^2 = \tfrac{7}{12}r^2 - \tfrac{1}{6}r,\ 3(2n - r)^2 = 7r^2 - 2r,$$
$$21(2n - r)^2 + 1 = 49r^2 - 14r + 1.$$

This reduces to the Pell Equation $s^2-21t^2=1$ where $s=7r-1$ and $t=2n-r$.

If we let $A=\frac{1}{2}r(r+1)$ and $B=\frac{1}{6}r(r-1)$, then $n(n-r)=\frac{1}{6}r(2r+1)$ and $u=\frac{1}{3}r(r+2)$ and the first equation reduces to the same Pell Equation $s^2-21t^2=1$, where $s=7r+1$ and $t=2n-r$.

The equation $s^2-21t^2=1$ has the following infinite set of solutions in nonnegative integers.

$$s_{i+1} = 110s_i - s_{i-1}, \quad t_{i+1} = 110t_i - t_{i-1}$$
$$s_0 = 1, \quad t_0 = 0; \qquad s_1 = 55, \quad t_1 = 12.$$

Since $110 \equiv -2 \pmod{14}$ it can be seen that the values of s will be alternately congruent to $+1$ and $-1 \pmod{14}$ so that $s_i = 7r-1$ will yield an integral value of r when i is odd, $s_i = 7r+1$ will yield an integral value of r when i is even, and, furthermore, r will always be an even number. Since $n = \frac{1}{2}(t+r)$ and t is even, n is always an integer.

From (3)

$$x = \frac{-\{n(n-1) - m(m-1) - 2mn\} \pm u}{2r}.$$

For odd i, $mn = n(n-r) = \frac{1}{6}r(2r-1)$, $u = \frac{1}{3}r(r-2)$ and we get

$$x = -n + r \quad \text{or} \quad -n + \tfrac{2}{3}(r+1), \qquad z = r \quad \text{or} \quad \tfrac{2}{3}(r+1).$$

For even i, $mn = n(n-r) = \frac{1}{6}r(2r+1)$, $u = \frac{1}{3}r(r+2)$ and we get

$$x = -n + r + 1 \quad \text{or} \quad -n + \tfrac{1}{3}(2r+1), \qquad z = r + 1 \quad \text{or} \quad \tfrac{1}{3}(2r+1).$$

Thus for every solution of the Pell Equation $s^2 - 21t^2 = 1$ we get at least one pair of integral values of (x, z). For $s_1 = 55$, $t_1 = 12$, we get $r = 8$, $n = 10$ and $x = -n+r = -2$ or $= -n + \frac{2}{3}(r+1) = -4$.

$$z = r = 8 \quad \text{or} \quad \tfrac{2}{3}(r+1) = 6, \qquad m = n - r = 2,$$

so that

$$(-2)^2 + \cdots + 7^2 = 8^2 + 9^2 \quad \text{and} \quad (-4)^2 + \cdots + 5^2 = 6^2 + 7^2.$$

For $s_2 = 6049$, $t_2 = 1320$, we get $r = 864$, $n = 1092$ and

$$x = -n + r + 1 = -227, \qquad z = r + 1 = 865, \qquad m = n - r = 228,$$

so that

$$(-227)^2 + \cdots + 864^2 = 865^2 + \cdots + 1092^2.$$

If we take A and B as quadratics in r, $n(n-r) = \frac{1}{2}(A+B)$ will always reduce to an equation of type (4); some of these will have solutions, others will not. There are, of course, other possible values of A and B, and in particular cases r, $r-1$, or $r+1$ might themselves be broken up into integral factors. In all cases, since $n(n-r) = \frac{1}{2}(A+B)$, $r^2 + 2(A+B)$ must be a square.

A few other small values of r which yield solutions are: $r = 18$, which yields the solution $(-14)^2 + \cdots + 10^2 = 11^2 + \cdots + 17^2$ and $r = 25$, which yields the solutions $(-20)^2 + \cdots + 14^2 = 15^2 + \cdots + 24^2$ and $4^2 + \cdots + 38^2 = 39^2 + \cdots + 48^2$.

References

1. Brother U. Alfred, Consecutive integers whose sum of squares is a perfect square, this MAGAZINE, 37(1964) 19–32.

2. ———, Solution to Problem 550, this MAGAZINE, 37(1964) 359.

3. A. O. Gelfond, The solution of equations in integers, Translated from the Russian by Leo F. Boron, P. Noordhoff, Groningen, the Netherlands, 1960.

CIRCLES INSCRIBED IN TWO INTERSECTING CIRCLES

LEON BANKOFF, Los Angeles, California

In the figure, the radius of circle (O) is 1 and the radius of circle (P) is $\frac{1}{2}\sqrt{2}$, so the radius of (Q) is $\frac{1}{2}(\sqrt{2}-1)$. Then the radius, r, of the upper shaded circle (R) may be obtained from triangle OQR by Stewart's Theorem:

$$(OR)^2(PQ) + (RQ)^2(PO) = (RP)^2(OQ) + (PO)(PQ)(OQ)$$

or

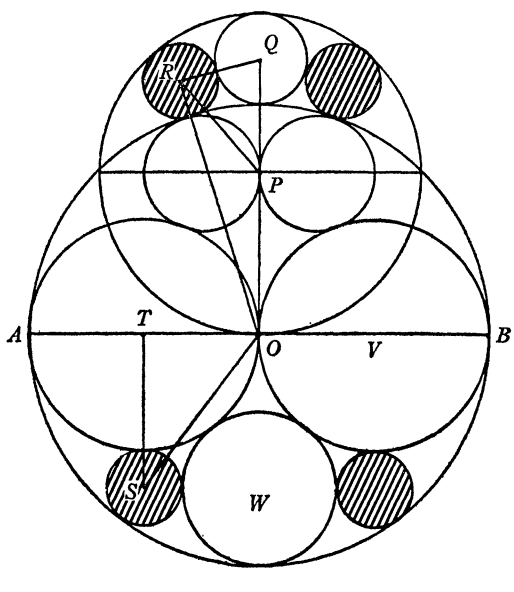
$$(1 + r)^2(1/2) + [1/2(\sqrt{2} - 1) + r]^2(1/2\sqrt{2})$$
$$= (1/2\sqrt{2} - r)^2(\sqrt{2} + 1)/2 + (1/2\sqrt{2})(1/2)(\sqrt{2} + 1)/2$$

which reduces to $r=1/6$.

Furthermore, (W) is the first and the lower shaded circle (S) is the second of a chain of circles whose radii, ρ_n, are given by the formula $\rho_n=R_1R_2R_3/(R_1R_2+n^2R_3^2)$ where R_1, R_2, R_3 are the radii of (O), (T) and (V), respectively. There fore the radius of (S) is

$$\rho = (1)(1/2)(1/2)/[(1)(1/2) + 2^2(1/2)^2] \text{ or } 1/6.$$

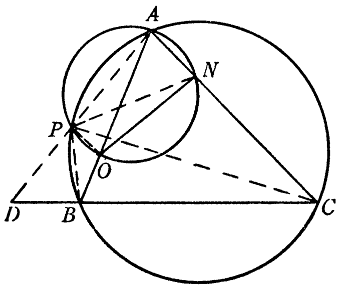
Consequently $r=\rho$ and the four shaded circles are equal.



RADICAL AXIS OF TWO CIRCLES

D. MOODY BAILEY, Princeton, West Virginia

Let N and O be points on sides CA and AB of triangle ABC and construct circles ABC and ANO to meet again at point P. AP is then the radical axis of circles ABC and ANO and may be extended to meet BC at point D.



The angles POA and PNA are equal since both are inscribed in circle ANO. This means that $\angle POB = \angle PNC$. Again, $\angle PBO = \angle PCN$ as both angles are inscribed in circle ABC. Triangles PBO and PCN are then similar since two angles of one equal two angles of the other. As a consequence $BO/CN = PO/PN$. Now PO and PN are chords of circle ANO and, if d be the diameter of this circle, it is known that

$$\frac{PO}{PN} = \frac{d \sin \angle PAO}{d \sin \angle PAN} = -\frac{\sin \angle OAP}{\sin \angle PAN} = -\frac{\sin \angle BAD}{\sin \angle DAC}.$$

So

$$\frac{\sin \angle BAD}{\sin \angle DAC} = -\frac{PO}{PN} = -\frac{BO}{CN}.$$

Let sides CA and AB of triangle ABC be represented by b and c. Application of the law of sines to the triangles ABD, ABC, and ADC yields $BD/DC = c/b \cdot \sin \angle BAD/\sin \angle DAC$ and substitution gives $BD/DC = -c/b \cdot BO/CN$. The ratio BO/CN may be written as

$$\frac{BO}{CN} = \frac{c}{b} \cdot \frac{b}{CN} \cdot \frac{BO}{c} = \frac{c}{b} \cdot \frac{\frac{b}{CN}}{\frac{c}{BO}} = \frac{c}{b}\left[\frac{\frac{CN+NA}{CN}}{\frac{BO+OA}{BO}}\right] = \frac{c}{b}\left[\frac{1+\frac{NA}{CN}}{1+\frac{OA}{BO}}\right]$$

$$= \frac{c}{b}\left[\frac{\frac{AN}{NC}+1}{\frac{AO}{OB}+1}\right].$$

A substitution of this value of BO/CN in the equation $BD/DC = -c/b \cdot BO/CN$ yields

$$\frac{BD}{DC} = -\frac{c^2}{b^2}\left[\frac{\dfrac{AN}{NC}+1}{\dfrac{AO}{OB}+1}\right].$$

THEOREM. *Let N and O be points on sides CA and AB of triangle ABC. The radical axis of circles ABC and ANO meets BC at D so that*

$$\frac{BD}{DC} = -\frac{c^2}{b^2}\left[\frac{\dfrac{AN}{NC}+1}{\dfrac{AO}{OB}+1}\right].$$

In using this theorem it must be remembered that the segments involved are to be treated as directed quantities. If N lies between C and A, then AN/NC is to be considered positive. If N lies on CA extended, then AN/NC is considered negative. Similar comments hold for the other ratios involved in the result given.

If M, N, O are collinear points on sides BC, CA, AB of triangle ABC, then it is possible to use this theorem to show that the radical axes of the pairs of circles ABC, $ANO-BCA$, $BOM-CAB$, CMN are concurrent. The point of concurrency may be shown to lie on circle ABC.

Let P be any point in the plane of triangle ABC and let MNO be its cevian triangle. The theorem may then be used to show that the radical axes of the pairs of circles ABC, ANO and BCA, BOM and CAB, CMN meet sides BC, CA, AB at three collinear points. Proof of these statements will be left as exercises for the reader interested in the geometry of the triangle.

$\int \sec^3 x dx$

JOSEPH D. E. KONHAUSER, HRB-Singer, Inc.

The standard method for evaluating $\int \sec^3 x dx$ is integration by parts. An alternative method is as follows:

$$\int \sec^3 x dx = \tfrac{1}{2}\int (\sec^3 x + \sec^3 x)dx = \tfrac{1}{2}\int (\sec^3 x + \sec x \tan^2 x + \sec x)dx$$

$$= \tfrac{1}{2}\int d(\sec x \tan x) + \tfrac{1}{2}\int \sec x dx$$

$$= \tfrac{1}{2}\sec x \tan x + \tfrac{1}{2}\ln(\sec x + \tan x) + C.$$

A substitution of this value of BO/CN in the equation $BD/DC = -c/b \cdot BO/CN$ yields

$$\frac{BD}{DC} = -\frac{c^2}{b^2}\left[\frac{\dfrac{AN}{NC}+1}{\dfrac{AO}{OB}+1}\right].$$

THEOREM. *Let N and O be points on sides CA and AB of triangle ABC. The radical axis of circles ABC and ANO meets BC at D so that*

$$\frac{BD}{DC} = -\frac{c^2}{b^2}\left[\frac{\dfrac{AN}{NC}+1}{\dfrac{AO}{OB}+1}\right].$$

In using this theorem it must be remembered that the segments involved are to be treated as directed quantities. If N lies between C and A, then AN/NC is to be considered positive. If N lies on CA extended, then AN/NC is considered negative. Similar comments hold for the other ratios involved in the result given.

If M, N, O are collinear points on sides BC, CA, AB of triangle ABC, then it is possible to use this theorem to show that the radical axes of the pairs of circles ABC, $ANO-BCA$, $BOM-CAB$, CMN are concurrent. The point of concurrency may be shown to lie on circle ABC.

Let P be any point in the plane of triangle ABC and let MNO be its cevian triangle. The theorem may then be used to show that the radical axes of the pairs of circles ABC, ANO and BCA, BOM and CAB, CMN meet sides BC, CA, AB at three collinear points. Proof of these statements will be left as exercises for the reader interested in the geometry of the triangle.

$\int \sec^3 x dx$

JOSEPH D. E. KONHAUSER, HRB-Singer, Inc.

The standard method for evaluating $\int \sec^3 x dx$ is integration by parts. An alternative method is as follows:

$$\int \sec^3 x dx = \tfrac{1}{2}\int (\sec^3 x + \sec^3 x)dx = \tfrac{1}{2}\int (\sec^3 x + \sec x \tan^2 x + \sec x)dx$$

$$= \tfrac{1}{2}\int d(\sec x \tan x) + \tfrac{1}{2}\int \sec x dx$$

$$= \tfrac{1}{2}\sec x \tan x + \tfrac{1}{2}\ln(\sec x + \tan x) + C.$$

RATIONAL TRIANGLES AND PARALLELOGRAMS

D. E. DAYKIN, The University, Reading, England

A polygon is said to be rational if the lengths of all its sides and diagonals are rational numbers. Prof. I. Schoenberg has asked whether rational polygons are everywhere dense in the class of all polygons; that is whether there exists a rational polygon whose sides and diagonals have lengths arbitrarily near to those of any given polygon. In [1] Prof. A. S. Besicovitch proved the following two theorems.

THEOREM 1. *The class of rational right-angled triangles is everywhere dense in the class of all right-angled triangles.*

THEOREM 2. *The class of rational parallelograms is everywhere dense in the class of all parallelograms.*

The object of this note is to extend Theorem 1 to Theorem 3 below and give a new simple proof of Theorem 2. In the proofs degenerate cases are ignored.

THEOREM 3. *If the angle θ has a rational cosine, then the class of rational triangles with θ as one angle is everywhere dense in the class of all triangles with θ as one angle.*

Proof of Theorem 3. If

$$(1) \qquad a = r\{s^2 - \cos^2\theta + 1\}, \qquad b = 2rs, \qquad c = r\{(s + \cos\theta)^2 - 1\}$$

then

$$(2) \qquad r = \frac{c - a - b\cos\theta}{2(\cos^2\theta - 1)}, \qquad s = \frac{b}{2r},$$

and $a^2 = b^2 + c^2 - 2bc\cos\theta$, so that a, b, c form the sides of a triangle with θ as one angle. If we are given such a triangle T we obtain corresponding real values r', s' for r, s from (2). Then to find a rational triangle whose sides have lengths which differ from those of the sides of T by less than some specified amount we simply have to choose rational values r'', s'' for r, s sufficiently close to r', s' and substitute them in (1).

Proof of Theorem 2. It is easy to show that the real numbers w, x and y, z form the sides and diagonals respectively of a parallelogram if and only if $2(w^2 + x^2) = y^2 + z^2$. Moreover if

$$(3) \quad a = \frac{2sr}{r^2 + 1}, \qquad b = \frac{s(r^2 - 1)}{r^2 + 1}, \qquad c = \frac{s(t^2 + 2t - 1)}{t^2 + 1}, \qquad d = \frac{s(t^2 - 2t - 1)}{t^2 + 1}$$

then

$$(4) \quad r = \frac{b + \sqrt{(a^2 + b^2)}}{a}, \qquad s = \frac{a(r^2 + 1)}{2r}, \qquad t = \frac{c + d + \sqrt{(2c^2 + 2d^2)}}{c - d}$$

and $a^2+b^2=s^2$, $c^2+d^2=2s^2$, so that a, b, c, d define a parallelogram. Given a parallelogram P we obtain real values r', s', t' for r, s, t from (4). Then to find a rational parallelogram whose sides and diagonals have lengths which differ from those of P by less than some specified amount we simply choose rational values r'', s'', t'' for r, s, t sufficiently close to r', s', t' and substitute in (3).

Reference

1. A. S. Besicovitch, Rational polygons, Mathematika, 6 (1959) 98.

ANSWERS

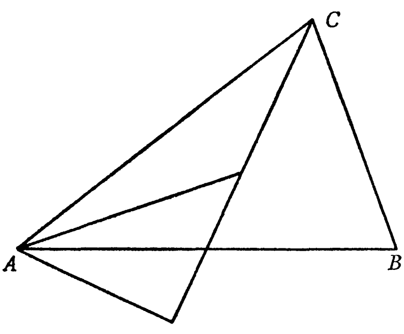
A349. It follows that

$$r_i + r_j = \sqrt{((x_i - x_j)^2 + (y_i + y_j)^2 + (z_i + z_j)^2)} = a_{ij}.$$

Whence $2r_i+\sum_1^4 r_i=a_{12}+a_{13}+a_{14}$, $\sum_1^4 r=\frac{1}{3}\sum_{r,s} a_{rs}$, $6r_1=2(a_{12}+a_{13}+a_{14})-(a_{23}+a_{34}+a_{42})$ and similarly for the other radii.

A350. If $n(n+2)(n+4)(n+6)=m^2$, then $(n^2+6n+4)^2=m^2+16$. But only 0 and 9 are squares of the form a^2-16, and since m^2 is odd, it must be $9=(-3)(-1)(1)(3)$.

A351. Construct a triangle with sides equal to 2/3 of the medians. From one vertex, A, draw a line to the midpoint of the opposite side and extend it a distance equal to its own length to B. Extend the side a distance equal to its own length to C. The required triangle is ABC.



A352. $U'(x)=U'(-x)$ implies $\int_{-x}^0 U'(x)dx=\int_0^x U'(x)dx$. Thus $U(0)-U(-x)=U(x)-U(0)$, or $U(x)+U(-x)=2U(0)$ and $U(x)=U(0)=C$.

A353. Differentiating with respect to x and then with respect to y yields

$$\frac{f''(x+y)}{f(x+y)}=\frac{f''(x-y)}{f(x-y)}=\text{constant}.$$

Whence $f(x)=a \sin mx$, ax, or $a \sinh mx$. This is a sort of a converse to Trickie T52 by C. F. Pinzka (Vol. 35, No. 2, March, 1962).

(Quickies on page 60)

BOOK REVIEWS

EDITED BY DMITRI THORO, San Jose State College

Materials intended for review should be sent to: Dmitri Thoro, Department of Mathematics, San Jose State College, San Jose, California 95114.

IBM 1620 Programming for Science and Mathematics. By I. A. Dodes. Hayden, New York, 1963. ix+276 pp. $5.96.

This book by the chairman of the Mathematics Department of the Bronx High School of Science is of interest primarily to those who have access to a 1620 computer. The contents are divided into four sections, the first being a very brief summary (40 pages) of some procedures in numerical analysis. Part two (86 pages) contains machine language programming. Part three (76 pages) is devoted to the symbolic programming system, SPS. In part four (61 pages) one finds FORTRAN with format. The Appendices which follow contain helpful summaries of operating procedures. Throughout the book the author has included many techniques which are the result of his own programming experience. There are flow charts, program listings, and examples illustrating applications of mathematics to science.

"IBM 1620 Programming" is dedicated to Thomas J. Watson. The author's point of view is set forth in his Introductory Remarks: "However, it is our opinion that it is impossible to understand symbolic language unless machine language is first understood. The idea that the computing machine is a 'black box' into one side of which a problem is inserted and from the other side of which the correct solution appears is the purest nonsense."

The book contains a number of misprints not included in the Errata inside the back cover. For example, on page 97, figure 24 line 1, "15006" should clearly read "15056." On page 47, the first sentence describing the IBM Sorter, reads "In this machine, most of the cards used in mathematical and scientific programming are keypunched with consecutive numbers in card columns 76 to 80." This sentence is certainly misleading. The Sorter does not keypunch cards.

Because it is so machine oriented "IBM 1620 Programming" is not an introduction to the overall field of computing. However, anyone who has a 1620 will probably want to look over Dodes' book. Planned as a basic text in programming the 1620, it is designed for advanced 12th grade or for junior college students. Many teachers may wish a larger fraction of the text were devoted to FORTRAN because it is essentially machine independent.

ALEXANDRA FORSYTHE, Cubberley High School, Palo Alto

University Mathematics. By Robert C. James. Wadsworth, Belmont, California, 1963. 924 pp. $13.50.

This book covers in a unified way the bulk of the material that might be found in any of the courses in mathematics ordinarily taught in the first two and a half years of college. It is designed to be used for two to two and a half years but could, with some difficulty in picking and choosing, be used as a text in standard courses.

BOOK REVIEWS

EDITED BY DMITRI THORO, San Jose State College

Materials intended for review should be sent to: Dmitri Thoro, Department of Mathematics, San Jose State College, San Jose, California 95114.

IBM 1620 Programming for Science and Mathematics. By I. A. Dodes. Hayden, New York, 1963. ix+276 pp. $5.96.

This book by the chairman of the Mathematics Department of the Bronx High School of Science is of interest primarily to those who have access to a 1620 computer. The contents are divided into four sections, the first being a very brief summary (40 pages) of some procedures in numerical analysis. Part two (86 pages) contains machine language programming. Part three (76 pages) is devoted to the symbolic programming system, SPS. In part four (61 pages) one finds FORTRAN with format. The Appendices which follow contain helpful summaries of operating procedures. Throughout the book the author has included many techniques which are the result of his own programming experience. There are flow charts, program listings, and examples illustrating applications of mathematics to science.

"IBM 1620 Programming" is dedicated to Thomas J. Watson. The author's point of view is set forth in his Introductory Remarks: "However, it is our opinion that it is impossible to understand symbolic language unless machine language is first understood. The idea that the computing machine is a 'black box' into one side of which a problem is inserted and from the other side of which the correct solution appears is the purest nonsense."

The book contains a number of misprints not included in the Errata inside the back cover. For example, on page 97, figure 24 line 1, "15006" should clearly read "15056." On page 47, the first sentence describing the IBM Sorter, reads "In this machine, most of the cards used in mathematical and scientific programming are keypunched with consecutive numbers in card columns 76 to 80." This sentence is certainly misleading. The Sorter does not keypunch cards.

Because it is so machine oriented "IBM 1620 Programming" is not an introduction to the overall field of computing. However, anyone who has a 1620 will probably want to look over Dodes' book. Planned as a basic text in programming the 1620, it is designed for advanced 12th grade or for junior college students. Many teachers may wish a larger fraction of the text were devoted to FORTRAN because it is essentially machine independent.

ALEXANDRA FORSYTHE, Cubberley High School, Palo Alto

University Mathematics. By Robert C. James. Wadsworth, Belmont, California, 1963. 924 pp. $13.50.

This book covers in a unified way the bulk of the material that might be found in any of the courses in mathematics ordinarily taught in the first two and a half years of college. It is designed to be used for two to two and a half years but could, with some difficulty in picking and choosing, be used as a text in standard courses.

The exposition is complete and detailed, and there are many historical remarks interspersed throughout. There are relatively few oddities in notation, and these are not radical departures. The language is the language of set theory and is thus "modern." There are many good problem sets.

I have some reservations about the use of the book as a classroom text. These stem primarily from the fact that so much is here written that is normally spoken by the teacher that the teacher in using the book as a text may find it hard to break away from the book not only in his formal presentations but also in his asides.

The author is clearly dedicated to good teaching and has spent a good deal of effort to make the exposition clear and attractive. Anyone interested in such a unified course or in new ways of presenting standard material would do well to examine this book whether or not he decides to use it as a text.

One final remark on the format is in order. The type is small, the margins narrow, and the book heavy. Successful study of a mathematics book depends more than is generally realized on the makeup of the page. It would have been far better to have larger type, wider margins, and to have made the book into two volumes.

J. B. ROBERTS, Reed College

Computers and Thought. Edited by Edward A. Feigenbaum and Julian Feldman. McGraw-Hill, New York, 1964. xiv+535 pp. $7.95.

To the mathematician, the computer is first of all an extension of the slide rule and the desk calculator—an extremely powerful tool for solving differential and algebraic equations, optimization problems, and a myriad of engineering design problems. But the computer can also extend the human intellect in solving nonnumerical problems of wide general interest. This is the aspect emphasized in *Computers and Thought*, a compilation of twenty papers which includes the pioneering work of Turing, who first suggested an operational method for answering the question, "Can a machine think?" Expanding the answers to that question, in effect, some papers discuss machines which can learn from experience—to play chess and checkers, for example, and to recognize patterns; other papers describe computer models of human thought and of elementary social behavior. Students of mathematics may be particularly interested in reading about machine solution of symbolic integration problems in freshman calculus and proofs of theorems in elementary Euclidean plane geometry. Two survey articles round out this collection: the first reviews the attitudes of Western and Russian scientists toward intelligent machines; the second provides a comprehensive overview of artificial intelligence research. Included also is a bibliography of approximately 1000 citations, cross-referenced by a descriptor index. Authoritative presentations and a well-chosen range of subjects make this book not only a valuable reference for the computer specialist, but an excellent introduction for the nonspecialist to a field of rapidly growing importance.

ROGER M. SIMONS, IBM Corporation, Los Gatos, California

The exposition is complete and detailed, and there are many historical remarks interspersed throughout. There are relatively few oddities in notation, and these are not radical departures. The language is the language of set theory and is thus "modern." There are many good problem sets.

I have some reservations about the use of the book as a classroom text. These stem primarily from the fact that so much is here written that is normally spoken by the teacher that the teacher in using the book as a text may find it hard to break away from the book not only in his formal presentations but also in his asides.

The author is clearly dedicated to good teaching and has spent a good deal of effort to make the exposition clear and attractive. Anyone interested in such a unified course or in new ways of presenting standard material would do well to examine this book whether or not he decides to use it as a text.

One final remark on the format is in order. The type is small, the margins narrow, and the book heavy. Successful study of a mathematics book depends more than is generally realized on the makeup of the page. It would have been far better to have larger type, wider margins, and to have made the book into two volumes.

J. B. ROBERTS, Reed College

Computers and Thought. Edited by Edward A. Feigenbaum and Julian Feldman. McGraw-Hill, New York, 1964. xiv+535 pp. $7.95.

To the mathematician, the computer is first of all an extension of the slide rule and the desk calculator—an extremely powerful tool for solving differential and algebraic equations, optimization problems, and a myriad of engineering design problems. But the computer can also extend the human intellect in solving nonnumerical problems of wide general interest. This is the aspect emphasized in *Computers and Thought*, a compilation of twenty papers which includes the pioneering work of Turing, who first suggested an operational method for answering the question, "Can a machine think?" Expanding the answers to that question, in effect, some papers discuss machines which can learn from experience—to play chess and checkers, for example, and to recognize patterns; other papers describe computer models of human thought and of elementary social behavior. Students of mathematics may be particularly interested in reading about machine solution of symbolic integration problems in freshman calculus and proofs of theorems in elementary Euclidean plane geometry. Two survey articles round out this collection: the first reviews the attitudes of Western and Russian scientists toward intelligent machines; the second provides a comprehensive overview of artificial intelligence research. Included also is a bibliography of approximately 1000 citations, cross-referenced by a descriptor index. Authoritative presentations and a well-chosen range of subjects make this book not only a valuable reference for the computer specialist, but an excellent introduction for the nonspecialist to a field of rapidly growing importance.

ROGER M. SIMONS, IBM Corporation, Los Gatos, California

Experiments in Topology. By Stephen Barr. Thomas Y. Crowell Co., New York, 1964. 210 pp. \$3.50.

As is the case with most books on topology for nonmathematicians, this book places primary emphasis upon the combinatorial aspects (rubber sheet geometry, Möbius strips, knots, etc.) rather than upon point-set topology. It is commendable, however, that the last two of its eleven chapters introduce some of the concepts of point-set topology.

In writing a book on topology for the layman, an author has two very difficult problems: choice of material and choice of language to explain that material. In the first respect the author has chosen well; in the second respect the choice is not so happy. It is possible to be unpretentious without being ungrammatical, informal without being imprecise. Most of the unfortunately constructed explanations are, with some effort, capable of interpretation, but some will cause difficulty. For example, it seems to the reviewer that even the most mathematically naive would more quickly comprehend something like "Our measure of 'shortness' will be the ratio of the length of the final edge to the width." rather than the author's "By 'short' is meant short along one-half its final edge as compared to its width—the width of the edges that we join . . . ." (p. 40).

Such objections aside, however, this book presents many interesting topics at an elementary level. The proof of Euler's theorem on polyhedra, for example, is particularly appealing. A careful reading of this book will be rewarded by an appreciation of some of the important objectives of modern topology.

BRUCE TRUMBO, San Jose State College

Equalities and Approximations: With FORTRAN Programming. By R. D. Larsson. Wiley, New York, 1963. x+158 pp. \$5.50.

A FORTRAN Primer. By E. I. Organick. Addison-Wesley, Reading, Mass., 1963. 186 pp. \$3.95.

Introduction to Electronic Computers. By F. J. Gruenberger and D. D. McCracken. Wiley, New York, 1963. vii+170 pp. \$2.95.

These are three quite different books. Each is a good book, written by a competent author. Each book has evolved from actual classroom experience using real live students. Each is designed for students who have no previous computer experience. One might expect the three volumes to be very similar. They are not. The basic philosophies of these three texts reflect three very different solutions to a common problem.

The book by Gruenberger and McCracken starts with basic (numeric) machine language coding. The student faces simple problems in scaling and overflow early in his career. He also learns some important coding techniques rather early. By page 25 he has learned that the "obvious" method of attack is not necessarily the shortest or best and has discovered the advantages of second differencing in preparing a table of squares over multiplication. By page 60 he has used flow charts of several degrees of complexity and discussed looping and subroutines with appropriate work on linkages. He has even built and used a "random number generator." Gruenberger and McCracken then provide brief

Experiments in Topology. By Stephen Barr. Thomas Y. Crowell Co., New York, 1964. 210 pp. $3.50.

As is the case with most books on topology for nonmathematicians, this book places primary emphasis upon the combinatorial aspects (rubber sheet geometry, Möbius strips, knots, etc.) rather than upon point-set topology. It is commendable, however, that the last two of its eleven chapters introduce some of the concepts of point-set topology.

In writing a book on topology for the layman, an author has two very difficult problems: choice of material and choice of language to explain that material. In the first respect the author has chosen well; in the second respect the choice is not so happy. It is possible to be unpretentious without being ungrammatical, informal without being imprecise. Most of the unfortunately constructed explanations are, with some effort, capable of interpretation, but some will cause difficulty. For example, it seems to the reviewer that even the most mathematically naive would more quickly comprehend something like "Our measure of 'shortness' will be the ratio of the length of the final edge to the width." rather than the author's "By 'short' is meant short along one-half its final edge as compared to its width—the width of the edges that we join . . . ." (p. 40).

Such objections aside, however, this book presents many interesting topics at an elementary level. The proof of Euler's theorem on polyhedra, for example, is particularly appealing. A careful reading of this book will be rewarded by an appreciation of some of the important objectives of modern topology.

BRUCE TRUMBO, San Jose State College

Equalities and Approximations: With FORTRAN Programming. By R. D. Larsson. Wiley, New York, 1963. x+158 pp. $5.50.

A FORTRAN Primer. By E. I. Organick. Addison-Wesley, Reading, Mass., 1963. 186 pp. $3.95.

Introduction to Electronic Computers. By F. J. Gruenberger and D. D. McCracken. Wiley, New York, 1963. vii+170 pp. $2.95.

These are three quite different books. Each is a good book, written by a competent author. Each book has evolved from actual classroom experience using real live students. Each is designed for students who have no previous computer experience. One might expect the three volumes to be very similar. They are not. The basic philosophies of these three texts reflect three very different solutions to a common problem.

The book by Gruenberger and McCracken starts with basic (numeric) machine language coding. The student faces simple problems in scaling and overflow early in his career. He also learns some important coding techniques rather early. By page 25 he has learned that the "obvious" method of attack is not necessarily the shortest or best and has discovered the advantages of second differencing in preparing a table of squares over multiplication. By page 60 he has used flow charts of several degrees of complexity and discussed looping and subroutines with appropriate work on linkages. He has even built and used a "random number generator." Gruenberger and McCracken then provide brief discussions of interpretative systems, assembly systems (SPS), compilers, (FORTRAN), and of generators. These brief discussions are not intended to make the user proficient in either the writing of or the use of these various systems, but to present the basic ideas of what each is designed to accomplish. They fill their intended purpose. The book continues with excellent sections on more advanced problems (a few more outside references would be welcome here), debugging techniques, and discussions of other computer systems. This is an excellent book for a student who really wants to learn what modern computers are all about and has an IBM 1620 as a living example.

Organick has devoted his entire book to FORTRAN. If your objective is to write programs in the FORTRAN language this may well be the book for you. The text is carefully prepared to be applicable to a wide variety of different computer systems and carefully illustrated with seven worked out major problems. The book concludes with a forecast of the FORTRAN IV compiler and some of its features. For the student who wants to use the computer as a tool for engineering problems (and this may well be the bulk of current students) this book provides quick access to the powerful language of FORTRAN. Your reviewer is disappointed that Dr. Organick has not included a few remarks on the niceties of obtaining shorter programs and on the mathematical dangers and shortcomings of computer solutions in general. The program given on pages 122–123 to solve the quadratic equation $Ax^2+Bx+C=0$ would provide an excellent example of how easy it is for a correct program to give erroneous results. A discussion of what extensions need to be made in the program to take care of the possibility that both A and B are zero need not be lengthy, but would alert the student to the vital possibility of these "unusual cases" occurring in computer problems. The omission of a discussion of the *mathematical* limitations of this (or any other) program seems even more serious. Floating point arithmetic does not *solve* the problem of scaling—it merely substitutes a different set of difficulties for the more usual ones. The equation $x^2+400000x+21=0$ does *not* have $x=0$ as its solution, no matter what the computer program obtains. Since some readers will have "nonexpert" instructors, it would seem desirable to discuss some of the more obvious numerical traps which every computer sets for its users. In short, Dr. Organick has written an excellent book on FORTRAN language which should be most welcome to the profession.

Larsson has taken a completely different attack from either of the above authors. He assumes his reader is mathematically naive (but intelligent) and is interested in learning some mathematics as well as the basic principles of FORTRAN. He begins with work on group theory and some basic theorems concerning finite groups. He then discusses some of the elementary processes on matrices and by page 38 has worked up to the Gauss-Jordan process for solving systems of several equations in several unknowns. His examples and problems are limited to three equations and three unknowns. Chapter 3, page 46, begins with basic operations in FORTRAN programming. The fine points (which bring forth differences among the over two hundred versions of FORTRAN now available) are left for the individual lab instructor or lecturer to discuss, but in general, Dr. Larsson does an excellent job of setting up some reasonably difficult FORTRAN programs, particularly those dealing with inequalities. He discusses truncation problems and area (integration) problems. He does not hesitate to use the limit process even though he originally designed the book for use with high school and beginning college students. He handles inequalities in a deft way. Polynomial approximations of transcendental functions are also introduced with examples. Larsson does not go into the fine details of approximation theory, but a deft teacher will find ample material to whet the appetites of even fairly advanced students of this new branch of applied mathematics. Larsson's treatment of FORTRAN is not as extensive as that of Dr. Organick, but he does discuss the related mathematics.

In conclusion: There are three different philosophical approaches to the first course in computer programming. Each has its advantages and its advocates. Your reviewer has tried all three methods at various times with various groups. Each philosophy produces desirable results, each has its drawbacks. As the old circus barker says, "You pays your money and you takes your choice."

A serious student of computer programming may well wish to order all three of these books for his bookshelf as well as for the library—at least I did.

R. V. ANDREE, University of Oklahoma

PROBLEMS AND SOLUTIONS

EDITED BY ROBERT E. HORTON, Los Angeles City College

Readers of this department are invited to submit for solution problems believed to be new that may arise in study, in research, or in extra-academic situations. Proposals should be accompanied by solutions, when available, and by any information that will assist the editor. Ordinarily, problems in well-known textbooks should not be submitted. Solutions should be submitted on separate, signed sheets. Send all communications for this department to Robert E. Horton, Los Angeles City College, 855 North Vermont Avenue, Los Angeles, California 90029.

PROPOSALS

572. *Proposed by Huseyin Demir, Middle East Technical University, Ankara, Turkey.*

To the memory of President Kennedy. Mr. J. F. Kennedy was killed on November 22, 1963. That is, on the day 11-22-1963. Solve the cryptarithm

$$JF\cdot(KEN+NEDY)=(11+22)\cdot 1963$$

in the decimal system.

573. *Proposed by Dewey Duncan, Los Angeles, California.*

A father bequeathed his herd of m horses to be divided among his sons, each son to receive an aliquot part of them. The specific divisions being impossible, a neighbor lends one horse to the herd which then made the prescribed partition possible, leaving the neighbor's horse untaken. Obtain all possible situations for:

reasonably difficult FORTRAN programs, particularly those dealing with inequalities. He discusses truncation problems and area (integration) problems. He does not hesitate to use the limit process even though he originally designed the book for use with high school and beginning college students. He handles inequalities in a deft way. Polynomial approximations of transcendental functions are also introduced with examples. Larsson does not go into the fine details of approximation theory, but a deft teacher will find ample material to whet the appetites of even fairly advanced students of this new branch of applied mathematics. Larsson's treatment of FORTRAN is not as extensive as that of Dr. Organick, but he does discuss the related mathematics.

In conclusion: There are three different philosophical approaches to the first course in computer programming. Each has its advantages and its advocates. Your reviewer has tried all three methods at various times with various groups. Each philosophy produces desirable results, each has its drawbacks. As the old circus barker says, "You pays your money and you takes your choice."

A serious student of computer programming may well wish to order all three of these books for his bookshelf as well as for the library—at least I did.

R. V. ANDREE, University of Oklahoma

PROBLEMS AND SOLUTIONS

EDITED BY ROBERT E. HORTON, Los Angeles City College

Readers of this department are invited to submit for solution problems believed to be new that may arise in study, in research, or in extra-academic situations. Proposals should be accompanied by solutions, when available, and by any information that will assist the editor. Ordinarily, problems in well-known textbooks should not be submitted. Solutions should be submitted on separate, signed sheets. Send all communications for this department to Robert E. Horton, Los Angeles City College, 855 North Vermont Avenue, Los Angeles, California 90029.

PROPOSALS

572. *Proposed by Huseyin Demir, Middle East Technical University, Ankara, Turkey.*

To the memory of President Kennedy. Mr. J. F. Kennedy was killed on November 22, 1963. That is, on the day 11-22-1963. Solve the cryptarithm

$$JF\cdot(KEN + NEDY) = (11 + 22)\cdot 1963$$

in the decimal system.

573. *Proposed by Dewey Duncan, Los Angeles, California.*

A father bequeathed his herd of m horses to be divided among his sons, each son to receive an aliquot part of them. The specific divisions being impossible, a neighbor lends one horse to the herd which then made the prescribed partition possible, leaving the neighbor's horse untaken. Obtain all possible situations for:

a) Two sons; e.g., 1/2, 1/3 of herd of five horses.

b) Three sons; e.g., 1/2, 1/3, 1/7 of herd of 41 horses.

c) A solution for n sons, each son to receive a different aliquot part of the herd.

574. *Proposed by Alan Sutcliffe, Kidsgrove, Stoke-on-Trent, Staffordshire, England.*

A bowl with a flat base is part of a sphere of internal radius 13 inches. The base of the bowl is a plane 7 inches below the center of the sphere. In it rest three smaller equal spheres, each of which touches the base of the bowl, the side of the bowl, and the other two spheres.

a) What is the radius of each of the small spheres?

b) Find complete solutions in integers for large bowl of radius R, small spheres of radius r, and base k units below the center of the sphere.

575. *Proposed by Fred Terry, Northwestern University.*

Objects labeled 1, 2, $\cdots$, 10 are arranged in a line from left to right in random order. 1 through 4 are red, and 5 through 10 are black. Let x equal the position number, counting from the left, in which a red object first appears.

a) Find $E(x)$ when drawing without replacement.

b) Solve by Difference Calculus only.

576. *Proposed by V. F. Ivanoff, San Carlos, California.*

A quadrangle with area Q is divided by its diagonals into four triangles with areas A, B, C, and D. Show that

$$A\cdot B\cdot C\cdot D=\frac{(A+B)^2(B+C)^2(C+D)^2(D+A)^2}{Q^4}.$$

577. *Proposed by Murray S. Klamkin, SUNY at Buffalo, New York.*

Show that if $x_n \geqq x_{n-1} \geqq \cdots \geqq x_2 \geqq x_1 \geqq 0$, then $x_1^{x_2}x_2^{x_3}\cdots x_n^{x_1} \geqq x_2^{x_1}x_3^{x_2}\cdots x_1^{x_n}$ for $n\geqq 3$, with equality holding only if $n-1$ of the numbers are equal.

578. *Proposed by Michael Gemignani, University of Notre Dame, Indiana.*

Let G be any group, and let $C=g_1A\cap g_2B$ where A and B are subgroups of G and g_1, $g_2\in G$. Prove there is a subgroup $D\subseteq G$ and $g_3\in G$ such that $C=g_3D$.

SOLUTIONS

Late Solutions

538, 544. *M. G. Murdeshwar, University of Alberta, Canada.* **550,** *Allan Chuck, San Francisco, California; M. N. Srikanta Swamy, University of Saskatchewan.*

Crystal Clear

551. [May, 1964] *Proposed by C. W. Trigg, San Diego, California.*

Reconstruct the following multiplication, given that $R=3$.

$$
\begin{array}{ccccccccccccc}
 & & & & & & & * & * & * & * & * & R \\
 & & & & & & R & * & * & * & * & * & * \\
\cline{7-13}
 & & & & & & R & * & R & * & R & * & C \\
 & & & & & & * & * & * & * & * & R & \\
 & & & & * & * & * & * & * & * & Y & & \\
 & & & & * & * & * & R & * & S & & & \\
 & & * & * & * & * & * & * & T & & & & \\
 & * & * & * & * & * & * & A & & & & & \\
C & R & Y & S & T & A & L & & & & & & \\
\hline
* & * & * & * & * & * & * & * & * & * & * & * & *
\end{array}
$$

Solution by C. C. Oursler, Southern Illinois University (Edwardsville).

We adopt the strategy of attempting to establish the digits in the multiplicand. Let us call the multiplicand $N=abcdeR$ and the multiplier $Rfghijk$. Some preliminary observations:

$L=R\cdot R=9$; j is 1; $3\cdot(abcdeR)=CRYSTAL$. N is a six-digit number, but $3N$ is a seven-digit number. Hence $C=1$ and $a=4$. Then the other six-digit multiple of N must be $2N$, thus $h=2$ and $S=6$. Since $C=1$, the third line shows that $k=7$.

From the sixth line, we have $(d\ e\ 3)\cdot 2\equiv 3\times 6 \pmod{1000}$. Since the hundreds digit is odd, there must be a carry-over from $2e$, hence $e=5$, 6, 7, 8, or 9; furthermore, the carry-over is exactly one, hence $2d+1\equiv 3 \pmod{10}$ and $d=1$ or 6.

Next we examine the third line, where we have either $(1\ e\ 3)\cdot 7\equiv 3\times 1$ (mod 1000) or $(6\ e\ 3)\cdot 7\equiv 3\times 1$ (mod 1000). In the second case, the carry-over from $7\ e+2$ must be 1, hence $e=2$, contradicting a previous observation about e. Hence, we must have $d=1$. Then, since $(1\ e\ 3)\cdot 7\equiv 3\times 1$ (mod 1000), the carry-over from $7\ e+2$ must be 6 and $e=9$. Thus, the terminal three digits of N must be 193, and, by the ninth line, $(4\ b\ c\ 193)\cdot 3=13\ Y\ 6\ 5\ 7\ 9$, hence $c=2$. Then, by line three, $(4\ b\ 2193)\cdot 7=3\times 3\ 5\ 3\ 5\ 1$, and we must have $b=6$.

Now, $N=4\ 6\ 2\ 1\ 9\ 3$, and, since $3N=1\ 3\ 8\ 6\ 5\ 7\ 9=CRYSTAL$, we obtain the missing capital letters. Comparison of the now-known terminal digits of the partial products shows immediately that the multiplier is 3 9 5 2 6 1 7 and the solution is complete.

Also solved by Philip Anderson, Montclair State College, New Jersey; Merrill Barneby, University of North Dakota; William Berlinghoff, The College of St. Rose, New York; Joseph B. Bohac, St. Louis, Missouri; Maxey Brooke, Sweeney, Texas; Sarah Brooks, Utica, New York; Philip Fung, Fenn College, Ohio; Harry M. Gehman, SUNY at Buffalo, New York; Murray Geller, Jet Propulsion Laboratory, Pasadena, California; Anton Glaser, Pennsylvania State University (Ogontz Campus); J. A. H. Hunter, Toronto, Ontario, Canada; Sidney Kravitz, Dover, New Jersey; Calvin C. Rice, Vestal, New York; Jerome J. Schneider, Chicago, Illinois; Polly and Sidney Spital, California State Polytechnic College (Jointly); Ira Sterbakov, Drexel Institute of Technology, Pennsylvania; Tom D. Turner, Seattle, Washington; Eugene Wermer, Northfield, Vermont; Sandra White, Mercer Island High School, Mercer Island, Washington; and the proposer.

Hunter mentioned that it is possible to derive as a necessary condition the fact that $R=3$.

Conditional Inequalities

552. [May, 1964] *Proposed by Yasser Dakkah, S. S. Boys School, Qalqilya, Jordan.*

Given a right circular cylinder with base of radius r, height h, volume V, and lateral area A. If $r+h=k$, a constant, prove:

$$1.\ V \leqq \frac{4\pi k^3}{27} \qquad 2.\ A \leqq \tfrac{1}{2}\pi k^2.$$

I. *Solution by Daniel L. Hansen, Westmar College, Iowa.*

1. Since $V=\pi r^2 h$, consider the arithmetic mean, A, of the three numbers $\frac{1}{2}r$, $\frac{1}{2}r$, and h. $A=(r+h)/3$ and the geometric mean, G, of these three is

$$G = \sqrt[3]{\left(\frac{r^2h}{4}\right)} = \left(\frac{V}{4\pi}\right)^{1/3}.$$

Now, since $k=r+h$, $A=k/3$ and since it is known that $G\leqq A$ we have

$$\left(\frac{V}{4\pi}\right)^{1/3} \leqq \frac{k}{3} \quad \text{or} \quad \frac{V}{4\pi} \leqq \frac{k^3}{27} \quad \text{and} \quad V \leqq \frac{4\pi k^3}{27}.$$

2. The lateral area A of the cylinder is $A=2\pi rh$. Starting with the inequality $(r-h)^2\geqq 0$ we add $4rh$ to both sides. Thus we obtain $(r+h)^2\geqq 4rh$. Multiply both sides by π and use the fact that $A=2\pi rh$ and $r+h=k$ to obtain

$$\pi k^2 \geqq 2A \quad \text{or} \quad A \leqq \tfrac{1}{2}\pi k^2.$$

II. *Solution by Michael J. Pascual, Watervliet Arsenal, New York.*

$$\begin{aligned} 1.\quad V(r) &= \pi r^2(k-r) \\ V'(r) &= 2\pi kr - 3\pi r^2 \\ V''(r) &= 2\pi k - 6\pi r \text{ and} \\ V'(r) &= 0 \quad \text{for} \quad r = \tfrac{2}{3}k, \end{aligned}$$

where $V''<0$ hence $V(\frac{2}{3}k)=4\pi k^3/27$ is a maximum.

$$\begin{aligned} 2.\quad A(r) &= 2\pi r(k-r) \\ A'(r) &= 2\pi k - 4\pi r \\ A''(r) &= -4\pi < 0 \\ A'(r) &= 0 \quad \text{for} \quad r = k/2 \end{aligned}$$

hence

$$A\left(\frac{k}{2}\right) = \frac{\pi k^2}{2} \text{ is a maximum.}$$

Also solved by Philip Anderson, Montclair State College, New Jersey; William E. F. Appuhn, Long Island University; Leon Bankoff, Los Angeles, California; William Berlinghoff, College of St. Rose, New York; Joseph B. Bohac, St. Louis, Missouri; Dermott A. Breault, Sylvania A.R.L., Waltham, Massachusetts; Robert Brodeur, Lacine, P.Q., Canada; Sarah Brooks, Utica, New York; Martin J. Brown, St. Xavier High School, Cincinnati, Ohio; Martin J. Cohen, Beverly Hills, California; R. J. Cormier, University of Missouri; Thomas Vanden Eynden, Kodiak High School, *Kodiak, Alaska; Brother Louis Francis, Archbishop Malloy High School, Jamaica, New York; Philip Fung, Fenn College, Ohio; Anton Glaser, Pennsylvania State University (Ogontz Campus); Gerald Goertzel, White Plains, New York; Harald A. Heckart, Illinois College; J. A. H. Hunter, Toronto, Ontario, Canada; Bruce W. King, SUNY at Buffalo, New York; John Koelzer, State University of Iowa; Joseph D. E. Konhauser, HRB-Singer, Inc., State College, Pennsylvania; Aaron Lieberman, Farmingdale, New York; M. J. Pascual (second solution), Watervliet Arsenal, New York; Stanton Philipp, Seal Beach, California; Lewis B. Robinson, Baltimore, Maryland (two solutions); Perry A. Scheinok, Hahnemann Medical College, Philadelphia, Pennsylvania; Jerome J. Schneider, Chicago, Illinois; Sidney Spital, California State Polytechnic College; Ira Sterbakov, Philadelphia, Pennsylvania; Joseph N. Thomas, Baltimore, Maryland; Charles W. Trigg, San Diego, California; Tom D. Turner, Seattle, Washington; Sandra White, Mercer Island High School, Mercer Island, Washington; and the proposer.*

Magic Square Determinant

553. [May, 1964] *Proposed by Daniel I. A. Cohen, Princeton University.*

Prove that the determinant of the n by n magic square formed from the numbers 1 to n^2 is divisible by n if n is odd and by n^2+1 if n is even.

Solution by F. D. Parker, SUNY at Buffalo, New York.

The sum of the entries of the determinant is $n^2(n^2+1)/2$, so that each column has a sum $s=n(n^2+1)/2$. We pre-multiply the matrix of the determinant by the square matrix M whose first row and main diagonal entries are all unity, whereas all other entries are zero. This is a unitary matrix so that the determinant of the product is the determinant of the original mtrix. This product has the value s everywhere in the first row. The other entries are unchanged by the pre-multiplication, hence the determinant is divisible by s. If n is odd, then $(n^2+1)/2$ is an integer, and the determinant is divisible by n. If n is even, $n/2$ is an integer and the determinant is divisible by n^2+1.

It is not necessary to hypothesize a magic square, for it is sufficient that either the column sums be equal or that the row sums be equal. In the latter case we *post-multiply* by the transpose of the same matrix.

Under the original hypothesis it is easy to show that the determinant is divisible by n^2 if n is odd.

Also solved by William E. F. Appuhn, Long Island University; Martin J. Cohen, Beverly Hills, California; Gerald Goertzel, White Plains, New York; H. W. Gould, West Virginia University; Yasuhiko Ikebe, University of Texas; Lawrence Satz, New York University; Sidney Spital, California State Polytechnic College; and the proposer.

Oblique Asymptote

554. [May, 1964] *Proposed by Joseph Verdina, Long Beach State College, California.*

Find the asymptote to the curve given by

$$y^3 - x^3 + ax^2 = 0.$$

Solution by William E. F. Appuhn, Long Island University.

Since this is an algebraic equation in polynomial form in x and in y, and since the coefficients of the highest degree terms in x and in y are the constants -1 and $+1$ respectively, there are no straight line asymptotes parallel to either axis of coordinates. If there is an asymptote it is either rectilinear and oblique to the axes or it is curvilinear. The oblique asymptote may be obtained quite readily in either of the following ways:

(1) $$y = x\left(1 - \frac{a}{x}\right)^{1/3} = x - \frac{a}{3} - \frac{1}{9}\frac{a^2}{x} - \cdots$$

descending powers of x. As $|x| \to \infty$, i.e., increases without bound, this equation approaches the limiting form of $y = x - a/3$ which is the required asymptote.

(2) Let $y = mx + K$ represent an oblique line which meets the given curve in at least two points. For the points of intersection we have (by substitution)

$$(m^3 - 1)x^3 + (3Km^2 + a)x^2 + 3K^2mx + K^3 = 0.$$

In order to have an asymptote, two roots of this equation must become infinite and hence, $m^3 - 1 = 0$ and $3Km^2 + a = 0$. These equations have the unique solution $m = 1$ and $K = -a/3$ so that the asymptote is, as before $y = x - a/3$.

Also solved by Merrill Barneby, University of North Dakota; Wray G. Brady, Washington and Jefferson College, Pennsylvania; Martin J. Cohen, Beverly Hills, California; R. J. Cormier, University of Missouri; Philip Fung, Fenn College, Ohio; Gerald Goertzel, White Plains, New York; Joseph D. E. Konhauser, HRB-Singer, Inc., State College, Pennsylvania; M. J. Pascual, Watervliet Arsenal, New York; Stanton Philipp, Seal Beach, California; Sidney Spital, California State Polytechnic College; William K. Viertel, SUNY, Art Institute, Canton, New York; Hazel S. Wilson, Jacksonville University, Florida; and the proposer.

A Triangular Inequality

555. [May, 1964] *Proposed by Kaidy Tan, Fukien Normal College, Foochow, Fukien, China.*

With O as any point on the median AM of a triangle ABC, produce BO and CO meeting AC and AB at E and F, respectively. If $AB > AC$, prove that $BE > CF$.

I. *Solution by Ned Harrell, Los Altos, California.*

By Ceva's theorem,

$$\frac{AF}{FB} \cdot \frac{BM}{MC} \cdot \frac{CE}{EA} = 1.$$

Since AM is a median, $BM = MC$ and $BM/MC = 1$. Hence

$$\frac{AF}{FB} \cdot \frac{CE}{EA} = 1 \quad \text{and} \quad \frac{AF}{FB} = \frac{EA}{CE}.$$

Thus FE divides AB and CA proportionally, and it follows that FE is parallel to BC.

It then follows that triangle COB is similar to triangle FOE and $FO/OC = OE/BO$. Also $BE/OB = CF/CO$.

In triangles BMA and CMA, angle AMB is opposite AB and angle CMA is opposite AC. Then, since $AB > AC$, it follows that $\measuredangle AMB > \measuredangle CMA$.

In triangles BMO and CMO, BO is opposite angle AMB and OC is opposite angle CMO. Hence $BO > OC$. Thus

$$BO \cdot \frac{BE}{BO} > OC \cdot \frac{CF}{CO} \quad \text{or} \quad BE > CF.$$

II. *Solution by Hazel S. Wilson, Jacksonville University, Florida.*

Set up a coordinate system with the origin at M. Let $B=(-a, 0)$, $C=(a, 0)$, $A=(b, c)$, and $O=(p, q)$. The equation of AM is $cx-by=0$. Since O is on AM, $q=pc/b$ and $O=(p, pc/b)$.

Now we have the following equations:

(1) BO: $p(cx-by)-aby+apc=0$,

(2) CO: $p(cx-by)+aby-apc=0$,

(3) AC: $cx-by+ay-ac=0$,

(4) AB: $cx-by-ay+ac=0$.

Solving (1) and (3) simultaneously will give the coordinates of E. E is the point $[(2pb-ap+ab)/(b+p), 2pc/(p+b)]$. Similarly, F is the point

$$[(2pb - ab + ap)/(b + p), 2pc/(b + b)].$$

Note: Since the coordinates of E and F are the same, it follows that the line FE is parallel to BC. Not used in this proof.

$$\overline{BE}^2 = (a^2b^2 + b^2p^2 + p^2c^2 + 2ab^2p)/(b + p)^2,$$
$$\overline{CF}^2 = (a^2b^2 + b^2p^2 + p^2c^2 - 2ab^2p)/(b + p)^2,$$
$$\overline{BE}^2 = CF^2 + (4ab^2p)/(b + p)^2.$$

Hence $BE > CF$.

Also solved by William E. F. Appuhn, Long Island University; Leon Bankoff, Los Angeles, California; Wray G. Brady, Washington and Jefferson College, Pennsylvania; Sarah Brooks, Syracuse University, New York; Philip Fung, Fenn College, Ohio; P. R. Nolan, Department of Education, Dublin, Ireland; Stanton Philipp, Seal Beach, California; Sidney Spital, California State Polytechnic College; Marion Walter, Cambridge, Massachusetts; and Hazel S. Wilson (second solution).

The Professor's Son

556. [May, 1964] *Proposed by Sidney Kravitz, Dover, New Jersey.*

Professor Adams wrote on the blackboard a polynomial, $f(x)$, with integer coefficients and said, "Today is my son's birthday, and when we substitute x equal to his age, A, then $f(A)=A$. You will also note that $f(0)=P$ and that P is a prime number greater than A." How old is Professor Adams' son?

Solution by Robert Brodeur, Lachine, P. Q., Canada.

The polynomial $f(x)$ written on the blackboard must be of the form

$$y = a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0. \tag{1}$$

Since $f(0)=P$, it follows that $a_0=P$, where P is a prime number greater than A. Since $f(A)=A$, equation (1) becomes

$$A - [a_nA^n + a_{n-1}A^{n-1} + a_{n-2}A^{n-2} + \cdots + a_1A] = P \tag{2}$$

when the terms are rearranged.

Since all coefficients are integers, it is obvious that all terms of equation (2) are integers since A and P are also integers. Furthermore A being an aliquot part of the left-hand side of equation (2), it follows that A must divide P. But since P is a prime number, the only value acceptable for A is 1.

Therefore Professor Adams' son is 1 year old.

Also solved by Philip Anderson, Montclair State College, New Jersey; William E. F. Appuhn, Long Island University; Joseph Arkin, Spring Valley, New York; Merrill Barneby, University of North Dakota; William Berlinghoff, College of St. Rose, New York; Wray G. Brady, Washington and Jefferson College, Pennsylvania; Dermott A. Breault, Sylvania ARL, Waltham, Massachusetts; Sarah Brooks, Utica, New York; J. L. Brown, Jr., and H. S. Piper, Jr. (jointly), Ordnance Research Laboratory, State College, Pennsylvania; Martin J. Cohen, Beverly Hills, California; R. J. Cormier, University of Missouri; Thomas V. Eynden, Kodiak High School, Kodiak, Alaska; David Finkel, Temple University; Philip Fung, Fenn College, Ohio; Anton Glaser, University of Pennsylvania (Ogontz Campus); Gerald Goertzel, White Plains, New York; Daniel L. Hansen, Westmar College, Iowa; J. A. H. Hunter, Toronto, Ontario, Canada; Yasuhiko Ikebe, University of Texas; Bruce W. King, SUNY at Buffalo, New York; Joseph D. E. Konhauser, HRB-Singer, Inc., State College, Pennsylvania; Sidney Kravitz, Dover, New Jersey; Aaron Lieberman, Narrick, New York; W. I. Nissen, Jr.; M. G. Murdeshwar, University of Alberta, Canada; P. R. Nolan, Department of Education, Dublin, Ireland; M. J. Pascual, Watervliet Arsenal, New York; Stanton Philipp, Seal Beach, California; Henry J. Ricardo, Fordham University; Stewart M. Robinson, Union College, New York; Lawrence Satz, New York University; Jerome J. Schneider, Chicago, Illinois; Jonathan Z. Shoher, University of California at Berkeley; David L. Silverman, Beverly Hills, California; Sidney Spital, California State Polytechnic College; Ira Sterbakov, Philadelphia, Pennsylvania; Charles W. Trigg, San Diego, California; Tom D. Turner, Seattle, Washington; and the proposer.

Schneider pointed out that as $f(A)=MA+P$ and $P=M'A$, then next year instead of comparing A with P, Professor Adams can simply state that A is even; then, from $P=M'A$, we have approximately the age $A=P=2$.

A Triangle Identity

557. [May, 1964] *Proposed by Roy Feinman, Rutgers University.*

Let A, B, and C be the vertex angles of any triangle. There exists an identity $F(\cos A, \cos B, \cos C)\equiv 0$ which is symmetric in $\cos A$, $\cos B$, and $\cos C$, and is of degree 2 in each of these. What is it?

I. *Solution by Gerald Goertzel, White Plains, New York.*

If a, b, c are the sides opposite the vertices A, B, and C respectively, then

$$\begin{aligned} -a + b\cos C + c\cos B &= 0 \\ a\cos C - b + c\cos A &= 0 \\ a\cos B + b\cos A - c &= 0. \end{aligned}$$

These equations in a, b, and c, have a nontrivial solution if, and only if, the determinant of the coefficients vanishes, whence

$$F = \begin{vmatrix} -1 & \cos C & \cos B \\ \cos C & -1 & \cos A \\ \cos B & \cos A & -1 \end{vmatrix} \equiv 0$$

or $F=\cos^2 A+\cos^2 B+\cos^2 C+2\cos A\cos B\cos C-1\equiv 0$ which is the required identity.

II. *Solution by L. Carlitz, Duke University.*

It follows from $\cos C = -\cos (A+B) = -\cos A \cos B + \sin A \sin B$ that $(\cos C + \cos A \cos B)^2 = (1-\cos^2 A)(1-\cos^2 B)$ and therefore

$$\cos^2 A + \cos^2 B + \cos^2 C + 2 \cos A \cos B \cos C = 1.$$

REMARK. It follows from $\tan C = -\tan (A+B)$ that

$$\tan A + \tan B + \tan C = \tan A \tan B \tan C.$$

These formulas are given by H. Dörrie: *Ebene und sphärische Trigonometrie*, pp. 132, 133.

Also solved by William E. F. Appuhn, Long Island University; Martin J. Cohen, Beverly Hills, California; Philip Fung, Fenn College, Ohio; Burt S. Holland, Harpur College; Joseph D. E. Konhauser, HRB-Singer, Inc., State College, Pennsylvania; W. I. Nissen, Jr.; Stanton Philipp, Seal Beach, California; Sidney Spital, California State Polytechnic College; Ira Sterbakov, Philadelphia, Pennsylvania; Charles W. Trigg, San Diego, California; and the proposer.

Konhauser located the identity in Hobson's "A Treatise on Plane and Advanced Trigonometry," Dover edition, page 57.

QUICKIES

From time to time this department will publish problems which may be solved by laborious methods, but which with the proper insight may be disposed of with dispatch. Readers are urged to submit their favorite problems of this type, together with the elegant solution and the source, if known.

Q349. Four spheres whose centers are at (x_n, y_n, z_n), $n=1, 2, 3, 4$ are mutually tangent externally. Find their radii.

[*Submitted by Murray S. Klamkin*]

Q350. What square is the product of four consecutive odd integers?

[*Submitted by David L. Silverman*]

Q351. Construct a triangle given the three medians.

[*Submitted by Charles W. Trigg*]

Q352. Prove that if $U(x) = U(-x)$ and $U'(x) = U'(-x)$, then $U(x) = C$.

[*Submitted by Myron Tepper*]

Q353. Solve the functional equation

$$f(x+y)f(x-y) = \{f(x)+f(y)\}\{f(x)-f(y)\}$$

given f has a second derivative.

[*Submitted by Murray S. Klamkin*]

(Answers on page 47)

and $a^2+b^2=s^2$, $c^2+d^2=2s^2$, so that a, b, c, d define a parallelogram. Given a parallelogram P we obtain real values r', s', t' for r, s, t from (4). Then to find a rational parallelogram whose sides and diagonals have lengths which differ from those of P by less than some specified amount we simply choose rational values r'', s'', t'' for r, s, t sufficiently close to r', s', t' and substitute in (3).

Reference

1. A. S. Besicovitch, Rational polygons, Mathematika, 6 (1959) 98.

ANSWERS

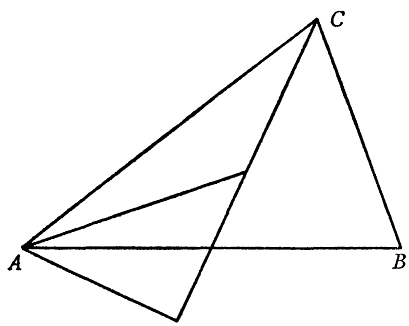
A349. It follows that

$$r_i + r_j = \sqrt{((x_i - x_j)^2 + (y_i + y_j)^2 + (z_i + z_j)^2)} = a_{ij}.$$

Whence $2r_i+\sum_1^4 r_i=a_{12}+a_{13}+a_{14}$, $\sum_1^4 r=\frac{1}{3}\sum_{r,s} a_{rs}$, $6r_1=2(a_{12}+a_{13}+a_{14})-(a_{23}+a_{34}+a_{42})$ and similarly for the other radii.

A350. If $n(n+2)(n+4)(n+6)=m^2$, then $(n^2+6n+4)^2=m^2+16$. But only 0 and 9 are squares of the form a^2-16, and since m^2 is odd, it must be $9=(-3)(-1)(1)(3)$.

A351. Construct a triangle with sides equal to 2/3 of the medians. From one vertex, A, draw a line to the midpoint of the opposite side and extend it a distance equal to its own length to B. Extend the side a distance equal to its own length to C. The required triangle is ABC.



A352. $U'(x)=U'(-x)$ implies $\int_{-x}^0 U'(x)dx=\int_0^x U'(x)dx$. Thus $U(0)-U(-x)=U(x)-U(0)$, or $U(x)+U(-x)=2U(0)$ and $U(x)=U(0)=C$.

A353. Differentiating with respect to x and then with respect to y yields

$$\frac{f''(x+y)}{f(x+y)}=\frac{f''(x-y)}{f(x-y)}=\text{constant}.$$

Whence $f(x)=a \sin mx$, ax, or $a \sinh mx$. This is a sort of a converse to Trickie T52 by C. F. Pinzka (Vol. 35, No. 2, March, 1962).

(Quickies on page 60)