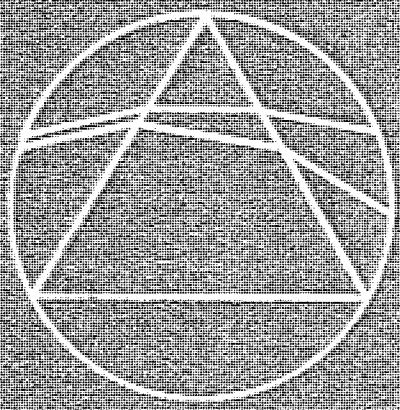
Mathematical Spectrum



Volume 10 1977/78 *Number* 1

A Magazine of *Contemporary Mathematics*

Published by the *Applied Probability Trust*

Mathematical Spectrum is a magazine for the instruction and entertainment of student mathematicians in schools, colleges and universities, as well as the general reader interested in mathematics. It is published by the Applied Probability Trust, a non-profit making organisation established in 1963 with the support of the London Mathematical Society. The object of the Trust is the encouragement of study and research in the mathematical sciences.

Volume 10 of *Mathematical Spectrum* will consist of three issues, the second of which will be published in January 1978, and the third in May 1978.

Articles published in *Mathematical Spectrum* deal with the entire range of mathematical disciplines (pure mathematics, applied mathematics, statistics, operational research, computing science, numerical analysis, biomathematics). Both expository and historical material may be included, as well as elementary research and information on educational opportunities and careers in mathematics. There is also a section devoted to problems. The copyright of all published material is vested in the Applied Probability Trust.

Articles are normally commissioned by the Editors; the Editorial Committee also welcomes the submission of suitable material, including correspondence, queries and solutions to problems, for publication in *Mathematical Spectrum*. All correspondence about the contents should be sent to:

The Editor, *Mathematical Spectrum*,
Hicks Building, The University, Sheffield S3 7RH.

Graphs and Convex Polygons

J. G. BRENNAN
University College of Swansea

In this article we shall establish a famous theorem of Euler (see Biographical Notes) about planar graphs and use it to solve some problems about convex polygons.

We have to begin with a number of definitions. A *graph*† consists of a finite, non-empty set of, say, V *vertices* together with a set of E *edges* joining some of these vertices in pairs, and subject to the conditions that

(i) no pair of vertices is joined by more than one edge,
(ii) each edge has distinct end-vertices.

Every graph may be represented by a figure in the plane, the vertices being represented by points and the edges by lines (not necessarily straight). A graph is called *planar* if it can be represented by a 'planar' figure; that is, one in which any two edges meet only at one of the V specified vertices.

Observe that the graph represented by the Figure 1 (in which only the four heavy dots represent vertices) is planar, since it can also be represented by the planar Figure 2.

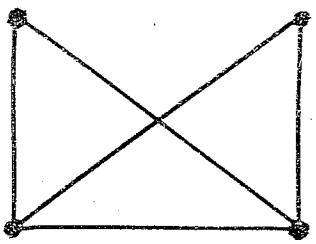


Figure 1

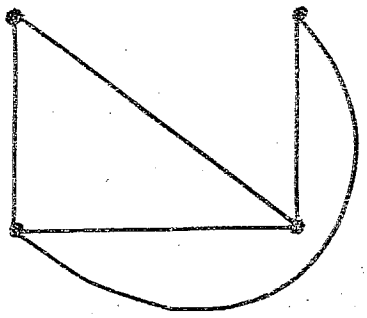


Figure 2

It suffices to give just one example to show that not all graphs are planar; thus no planar representation can be drawn for Figure 3, however ingeniously the edges are displaced.

A graph is *connected* if any two vertices may be joined by a 'path' consisting alternately of edges and vertices. For example, Figures 4 and 5 represent respectively a connected and a disconnected graph.

† The graphs described here are quite different from those which are drawn by plotting values of y against x to illustrate the behaviour of functions.

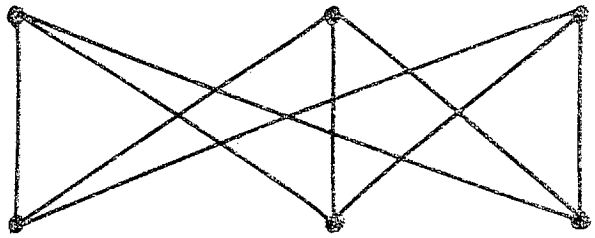


Figure 3

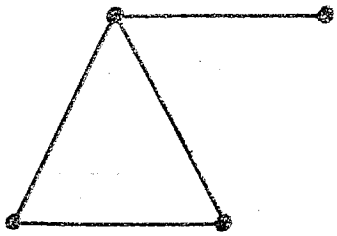


Figure 4

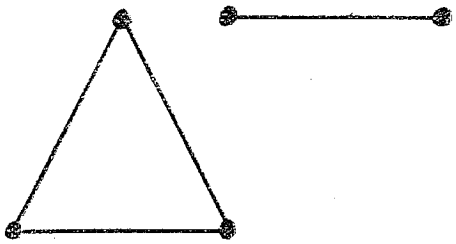


Figure 5

Let G be a planar graph, and suppose it is represented by a particular planar figure. The finite regions into which the edges in the figure divide the plane will be called the *faces* of that particular figure representing the graph. For the planar graph represented by Figure 6, $V = 7$, $E = 8$, and the figure has just $F = 2$

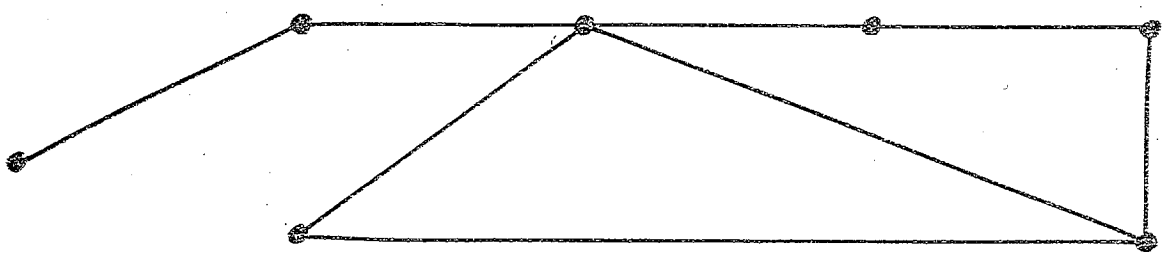


Figure 6

(triangular) faces. The faces themselves depend on the actual figure, but it is an interesting corollary of Euler's theorem below that their number F depends only upon the graph (since V and E depend only on the graph).

Euler's theorem. For any connected planar graph G and any representing (planar) figure, we have

$$F - E + V = 1.$$

(In Euler's original version of the theorem, a relation connecting the numbers of vertices, edges and faces of a convex polyhedron in space was stated. Our graph-theoretic formulation is obtained from this theorem by projection on to a plane, and is due to Cauchy (see Biographical Notes)).

The argument is by induction on the number of edges of G. If $E = 0$, then $V = 1$ ($V \not> 1$ since G is connected) and $F = 0$. Hence the theorem is true in this case.

Assume that $E > 1$ and that the theorem is true whenever G has $E - 1$ edges, and then add to G a further edge e. Either (i) e joins two distinct vertices of G, in which case the number of faces in any planar representation of G is increased by one and the number of vertices is left unchanged, or (ii) e is incident with only one vertex of G so that an extra vertex must be added to e. This increases the number of vertices by one and leaves the number of faces unchanged. In either case the theorem remains true and, since these are the only possible cases, the theorem is proved.

Consider now a convex plane polygon with vertices $P_1, P_2, \ldots, P_n$ which satisfies the following conditions:

(a) no three vertices P_i are collinear;

(b) no three diagonals are concurrent (except at a vertex of the original polygon).

The diagonals P_iP_j divide the interior of the polygon into a number F of convex regions each having a polygonal boundary.

Theorem 1.

$$F = \binom{n}{4} + \binom{n-1}{2}.$$

Let the total number of line segments comprising these boundaries (including the sides of the polygon) be denoted by E, and let the total number of points of intersection of the diagonals (including the vertices of the polygon) be denoted by V. The numbers F, E and V are related by Euler's equation

$$F = E - V + 1 \tag{1}$$

since the figure represents a connected planar graph.

To find V, we note that if four points chosen from $P_1, P_2, \ldots, P_n$ (forming a convex quadrangle) be joined in pairs in all possible ways, exactly one of the resulting intersections lies in the interior of the quadrangle. Indeed, just one lies inside the convex polygon $P_1, P_2, \ldots, P_n$ in Figure 7. This is an easy consequence of the fact that the line joining any two vertices X, Y of a convex polygon (adjacent or not) intersects its interior precisely in the segment XY. Each choice of four different vertices from $P_1, P_2, \ldots, P_n$ yields one such point. Hence, if we take account of the points $P_1, P_2, \ldots, P_n$ themselves, we have

$$V = \binom{n}{4} + n.$$

Just two vertices lie on each line-segment. On the other hand, each of the $\binom{n}{4}$ internal vertices lies on four line-segments while each of the n vertices P_i lies on $n - 1$ line-segments. Therefore, adding together the numbers of line-segments

through each vertex, we have

$$2E = 4\binom{n}{4} + n(n-1)$$

or

$$E = 2\binom{n}{4} + \binom{n}{2}.$$

Hence, from (1),

$$F = \binom{n}{4} + \binom{n-1}{2}.$$

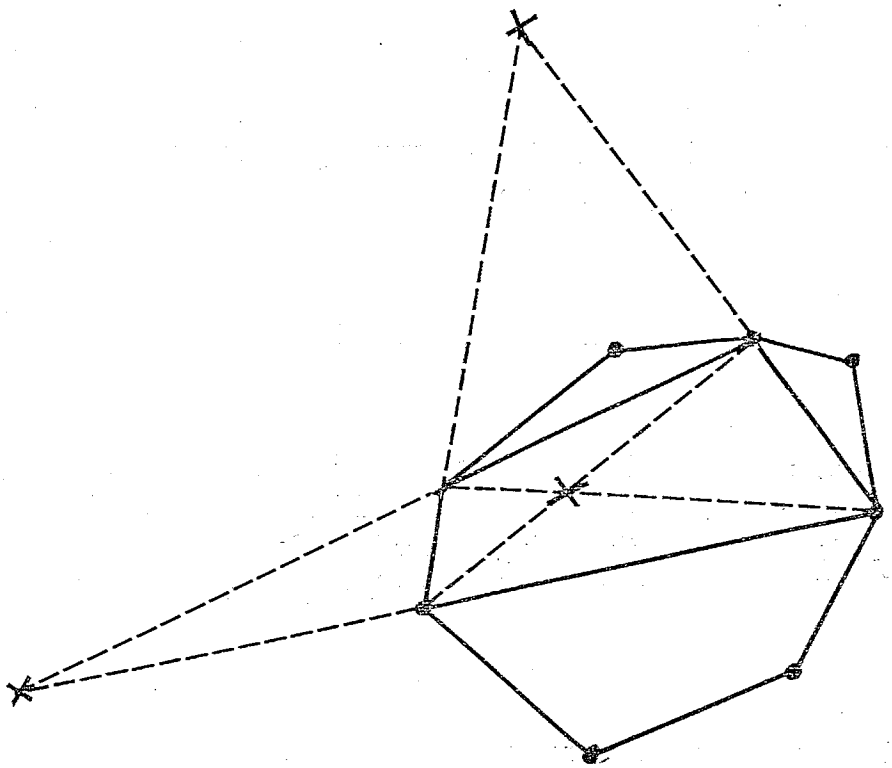


Figure 7

This problem was posed in reference 1 (Problem 47), and the proof which we have given is due to Murphy (reference 2).

It is natural to question what happens if either of the Conditions (a) or (b) is relaxed. The removal of (b) would take us too far afield, but we look briefly at the situation when (a) is relaxed for a single side of the polygon. Let, then, p further vertices $Q_1, Q_2, \ldots, Q_p$ be introduced in this order on the side P_1P_n of the polygon; let all the further diagonals P_iQ_j $(i = 2, 3, \ldots, n-1; j = 1, 2, \ldots, p)$ be drawn, and assume that the Condition (b) holds in regard to both sets of lines P_iP_j and P_iQ_j. Denote the resulting numbers of regions, segments and vertices by $F(n, p)$, $E(n, p)$ and $V(n, p)$ respectively.

Theorem 2.

$$F(n,p) = \binom{n+p}{4} + \binom{n+p-1}{2} - n\binom{p+2}{3} - \frac{1}{24}p(p+1)(p^2-7p-6).$$

The details of the calculation will be given only when $p = 1$ and $p = 2$. Readers may care to establish the general result for themselves by induction on p.

First, we observe that

$$F(n, 1) = \binom{n+1}{4} + \binom{n}{2} - (n - 1). \tag{2}$$

To see this, suppose that Q_1 is moved a very small distance from the line P_1P_n, say to Q'_1, in such a way that $P_1, P_2, \ldots, P_nQ'_1$ is a convex polygon (with $n + 1$ vertices) and let us make sure that the distance $Q_1Q'_1$ is so small that the Condition (b) holds for this new polygon. The number of regions inside it is equal to $F(n, 1) + (n - 1)$; and (2) follows from Theorem 1. Next, from (1),

$$F(n, 2) - F(n, 1) = E(n, 2) - E(n, 1) - [V(n, 2) - V(n, 1)]. \tag{3}$$

We have supposed that the point Q_1 has already been introduced and that all the corresponding diagonals have been drawn. Let us refer to all these lines as 'old lines'. Upon the introduction of Q_2 into the figure a number of 'new lines' $Q_2P_2, Q_2P_3, \ldots, Q_2P_{n-1}$ also arise. Let N be the number of points in the interior of the polygon which are intersections of new lines and old lines. Then

$$V(n, 2) - V(n, 1) = N + 1. \tag{4}$$

The introduction of Q_2 causes new segments to arise in three ways:

(i) one extra segment arises because Q_1Q_2 and Q_2P_n replace Q_1P_n,

(ii) a number R of new segments arise on the new lines,

(iii) N new segments arise on the old lines.

Hence

$$E(n, 2) - E(n, 1) = R + N + 1. \tag{5}$$

From (3), (4), (5), it follows that

$$F(n, 2) - F(n, 1) = R.$$

Now the number of new segments arising on Q_2P_i is

$$i(n - i - 1) + (i - 2) + 1 = i(n - i) - 1$$

for $2 \leqslant i \leqslant n - 1$; and so

$$R = \sum_{i=2}^{n-1} i(n - i) - (n - 2) = F(n, 2) - F(n, 1);$$

and this simplifies to give

$$F(n, 2) - F(n, 1) = \binom{n}{3} + \binom{n-2}{2}. \tag{6}$$

Finally, equations (3) and (6) furnish the value of $F(n, 2)$.

Biographical Notes

The famous Swiss mathematician Léonard Euler (1707–1783) was the son of a Calvinist pastor who was also a mathematician. Euler's first mathematical work was done at the age of 19. Most of his working life was spent at the Academies of St Petersburg and Berlin, and his mathematical output was prodigious. In 1752 Euler wrote two papers on the polyhedral formula. During the last 17 years of his life he was completely blind.

Augustin-Louis Cauchy (1789–1857) was the eldest of six children of a parliamentary lawyer. He grew up in France during the Terror following the French Revolution. The first of the 'modern' mathematicians, Cauchy was truly a pure mathematician who sought no immediate applicability for his researches. We owe to him in particular the origins of the theory of groups and the introduction of rigour into mathematical analysis.

References

1. A. M. Yaglom and I. M. Yaglom, *Challenging Mathematical Problems with Elementary Solutions*, Volume 1 (Holden-Day, San Francisco, 1964).
2. T. Murphy, The dissection of a circle by chords, *Math. Gazette* 56 (1972), 113–115.

Mathematics in the Service of Computer Programming

M. D. ATKINSON
University College, Cardiff

Most university and polytechnic mathematics courses include an opportunity for students to learn computer programming, i.e. the syntax and mechanics of a high-level language such as Algol, the concept of an algorithm and the recasting of algorithms as computer programs. Indeed, such topics are increasingly taught in schools, especially to students who are pursuing mathematically oriented subjects.

Now I believe that there is a natural association of computing with mathematics. This belief is reinforced every time I give an introductory programming course; there are plenty of trivial exercises relating to mathematics (e.g. quadratic equations, Newton–Raphson iteration, etc.) but one has to scratch one's head rather hard to find others. This paucity of simple non-mathematical programming exercises tends to give the impression that computers are merely handy servants for the working mathematician. This view of the relationship between computing and mathematics is very prevalent but, as I wish to show, it is not the whole story: there are situations

where these roles are reversed. I shall discuss two ways in which mathematics can be of use in programming.

Let us be rather lofty and ask: what does mathematics do for the world? If we virtuously ignore the possible material and monetary benefits, we could answer that it provides

(i) a collection of techniques for answering various naturally occurring questions,
(ii) a tradition of rigour which distinguishes it from the other sciences, and
(iii) knowledge for its own sake.

Now, by definition, we are not going to be able to make use of (iii), but within the last decade there have been two developments which harness (i) and (ii). Firstly, there has been an enormous spurt in the design and analysis of algorithms to solve commonly occurring problems. Moreover, this work goes far beyond the scope of the much older subject of numerical analysis. In these ideas heavy emphasis is placed on estimating the running time of an algorithm in terms of its parameters. Such estimates enable different algorithms for solving a problem to be compared; for example, if one had to sort n numbers into ascending order one would normally prefer an algorithm whose time of execution is of the order of $n \log n$ to one of order n^2. Many surprisingly fast algorithms have been discovered, and usually mathematical technique plays a large part in both the justification and the time analysis of these algorithms.

Secondly, the days when the correctness of a computer program was justified only by experiment and polemic seem to be numbered. As a result of the developments in programming methodology it is now possible to give formal and rigorous proofs that programs actually do what they purport to do. That is, if I wish to persuade you that my program works I will take you through its proof step by step as if it were a mathematical theorem, rather than prove it in the scientific experimental sense (i.e. running it with test data). You will emerge from this experience convinced of the correctness of the program, but possibly not with a full understanding of it; this also is akin to following through the proof of a theorem. As a consequence one can look forward to the day when programs can check their logic themselves.

I shall give some examples which, while extremely elementary, illustrate the above developments. The notation used in the example programs is 'Algol 68-ish'. The main points are the following.

(a) **if** *condition* **then** *action* **fi**. This causes the *action* to be performed if the *condition* is satisfied.

(b) **if** *condition* **then** *action* 1 **else** *action* 2 **fi**. This causes *action* 1 to be performed if the *condition* is satisfied and otherwise *action* 2 is performed.

(c) **while** *condition* **do** *action* **od**. This causes the *action* to be performed repeatedly so long as the *condition* remains satisfied (so if the *condition* is not satisfied initially the *action* is not performed at all).

(d) **for** *i* **from** *a* **to** *b* **by** *c* **do** *action* **od**. This causes the *action* to be performed repeatedly with i taking successively all those values $a, a + c, a + 2c, \ldots$ which do not exceed b.

The curious symbols **fi** and **od** are statement terminators and act like closing brackets to the opening brackets **if** and **do** respectively.

The first example concerns finding the maximum and minimum elements of a (linearly ordered) set of n distinct elements. How long should this take? To answer this question we must have a way of timing a program. Since it is difficult to imagine a program which does not do the job on the basis of comparing pairs of elements from the set, let us take the number of comparisons used as an estimate of the running time. Whether this is a good measure remains to be seen but it certainly provides us with a reasonable first approximation.

Of course, there is an obvious algorithm for solving the problem. We find the maximum and minimum independently. The maximum is found by 'remembering the largest so far' and the minimum is found similarly:

```
max := min := a(1);
for i from 2 to n by 1 do
    if max < a(i) then max := a(i) fi;
    if min > a(i) then min := a(i) fi od
```

This clearly requires $2(n - 1)$ comparisons.

On the other hand, it is possible to find both the maximum and the minimum in just $n - 1$ comparisons if we happen to have a great slice of luck. Suppose we compared $a(1)$ with $a(2)$, $a(2)$ with $a(3)$, ..., $a(n - 1)$ with $a(n)$ and in each case it happened that $a(i) < a(i + 1)$; then $a(1)$ would be the minimum and $a(n)$ would be the maximum. Of course, such good fortune will hardly ever happen to us but it does mean that when we ask how many comparisons a particular method requires we perhaps should cautiously add some phrase such as 'in the worst case' or 'on average'.

Some idea of how much we might hope to improve the algorithm above is provided by the following result.

Lemma. Any algorithm for finding the maximum and minimum requires in the worst case at least $3n/2 - 2$ comparisons if n is even and at least $3(n - 1)/2$ comparisons if n is odd.

Proof. At any point in the algorithm let the set of elements which are still possibilities for the maximum be denoted by A and the possibilities for the minimum be denoted by B. Then initially $|A| = |B| = n$† and the algorithm should terminate when $|A| = |B| = 1$. Consider a typical comparison of two elements x and y and the effect it has on A and B. If $x, y \in A \cap B$, then no matter whether $x > y$ or $y > x$ we can exclude an element from A and a different element from B and the

† The number of elements in a (finite) set X is denoted by $|X|$.

size of $A \cap B$ will be decreased by 2. It is easy to see that this is the only case in which both A and B are certain to be diminished. (Suppose, for example, that $y \notin B$ and it happens that $x > y$; then no further element can be excluded from B.) Since initially $A \cap B$ has size n, there will be $k \leqslant \frac{1}{2}n$ comparisons which diminish both A and B. Since any comparison only reduces the size of A or B by at most one, a further $2(n - k - 1)$ comparisons are required before A and B each have just one element. So the total number of comparisons is at least $2(n - k - 1) + k$, from which the result follows.

This lower bound is actually best possible because of the following algorithm. For clarity we give a version valid only for odd numbers n, but trivial modifications remove this restriction.

```
max := min := a(1);
for i from 3 to n by 2 do
    if a(i − 1) < a(i) then
        if max < a(i) then max := a(i) fi;
        if min > a(i − 1) then min := a(i − 1) fi
    else
        if max < a(i − 1) then max := a(i − 1) fi;
        if min > a(i) then min := a(i) fi
    fi
od
```

The idea of the algorithm is clear: keep a record of the largest and smallest elements so far, take a new pair and rank them, compare the larger with the current largest and the smaller with the current smallest to get new largest and smallest elements (cf. a set with two extra elements). It is clear that the number of comparisons is $3(n - 1)/2$.

Perhaps now is the time to examine our assumption about comparisons being a reasonable measure of the running time. We can compare the two algorithms we have had. Although the second is physically longer, it is fairly comparable to the first except in the number of comparisons; and indeed when subjected to the acid test of an actual computer run, it is slightly faster.

Our next example is similar: this time the problem is to find the largest and second largest of a set of size n. An approach similar to the one above accomplishes this in about $3n/2$ comparisons. This is an improvement over the obvious method of finding first the largest and then the largest of those elements remaining ($2n - 3$ comparisons), but it still is not optimal. Consider the following algorithm (in which $m1$ denotes the current largest, $m2$ the current second largest):

```
if a(1) > a(2) then m1 := a(1); m2 := a(2) else m2 := a(1); m1 := a(2) fi;
for i from 3 to n by 1 do
    if m2 < a(i) then
        if m1 < a(i) then m2 := m1; m1 := a(i) else m2 := a(i) fi
    fi
od
```

The basic idea is that, whenever we find some $a(i)$ which is smaller than $m2$, then we need not modify $m2$ or $m1$. Now there are some cases where this algorithm is not especially good. (For example, if $a(1) < a(2) < \cdots < a(n)$, it requires $2n - 3$ comparisons.) But it has a good expected running time which can be derived from the following simple probabilistic argument.

There are $n - 2$ comparisons of $m2$ with $a(i)$ and, whenever $m2 < a(i)$, a further comparison is made. Now $m1$ and $m2$ represent the largest and second largest elements found so far. Hence

$$\begin{aligned}\Pr(m2 < a(i)) &= \Pr(a(i) \text{ is the largest or second largest among } a(1), \ldots, a(i)) \\ &= 2/i.\end{aligned}$$

So the total expected number of comparisons is $1 + n - 2 + \Sigma_{i=3}^{n} 2/i$, which is approximately $n - 1 + 2(\log_e n + \gamma) - \frac{3}{2}$, where γ is Euler's constant.†

Actual computer runs confirm that this is indeed faster than the other two methods mentioned, and so again comparisons have been justified as the measure of time. There are, however, many problems where some other measure of running time is more appropriate.

Finally, we take a look at an example of program proving. Consider the following program (due to E. W. Dijkstra, reference 1) in which all the variables are integers, $n > 0$ is the input value and p is the result.

```
v := n; p := 0; q := 1;
while q ≤ n do q := 4 * q od;
while q ≠ 1 do
    q := q/4; h := p + q; p := p/2;
    if h ≤ v then p := p + q; v := v − h fi
od
```

Now I hope you will not think that the result of this program is obvious, even when I tell you that the final value of p is the integer part of $\sqrt{n}$. We are going to prove this.

The first line of the program has an obvious effect and the second line is also fairly clear: q is set to the smallest power of 4 which exceeds n. But it is in the second **while** loop that we are in doubt as to what is going on. The key concept is that of a *loop invariant* by which we mean an assertion whose truth is not destroyed by any single iteration of the loop. Thus, if the assertion is true initially, it is (by induction) true on exit from the loop.

We take the following assertion:

$$2p + q > v = n - p^2/q \geqslant 0.$$

This is certainly true before the second **while** loop is entered, for then $v = n, p = 0$ and $q > n$. It is also clear that this loop eventually terminates. (q is a power of 4,

† It may be shown that $(1 + \frac{1}{2} + \frac{1}{3} + \cdots + 1/n) - \log_e n$ tends to a limit as $n \to \infty$. This limit, usually denoted by γ, is called Euler's constant; its value is 0·5772 . . . .

is continually divided by 4 and so must reach 1.) If we can prove that the above assertion is a loop invariant, we shall have on exit

$$2p + 1 > n - p^2 \geqslant 0,$$

from which it follows that $p^2 \leqslant n < (p + 1)^2$ as required. So we have simply to establish that the assertion remains true when a typical iteration of the loop is performed.

Let p_0, q_0, v_0 be the values of p, q, v at the start of such a typical iteration and let p_1, q_1, v_1 be the values at the end of the typical iteration. In view of the **if** statement we must consider two cases corresponding to $h \leqslant v$ and $h > v$. In the case $h \leqslant v$ we have

$$q_1 = q_0/4, \quad h = p_0 + q_0/4 \leqslant v_0, \quad p_1 = p_0/2 + q_0/4, \quad v_1 = v_0 - (p + q_0/4).$$

Then $v_1 \geqslant 0$,

$$2p_1 + q_1 = p_0 + 3q_0/4 = 2p_0 + q_0 - (p_0 + q_0/4) > v_0 - (p_0 + q_0/4) = v_1$$

and

$$v_1 = v_0 - (p_0 + q_0/4) = n - p_0^2/q_0 - p_0 - q_0/4$$

$$= n - \frac{(p_0/2 + q_0/4)^2}{q_0/4} = n - p_1^2/q_1$$

as required. In the case $h > v$ we have

$$q_1 = q_0/4, \qquad h = p_0 + q_0/4 > v_0, \qquad p_1 = p_0/2, \qquad v_1 = v_0$$

and again it is routine to verify that the assertion remains true.

Note that the proof also shows that the division in $p := p/2$ always produces an integer result: a point which initially should have worried us.

Reference

1. E. W. Dijkstra, The composition of programs guided by their correctness proofs, Invited Lecture, Inter-Universities Computing Colloquium, University of Kent at Canterbury, 1973.

On Extracting Square Roots of Perfect-Square Numbers by Inspection

S. BOOKCHIN† and M. LEWIN
Technion–Israel Institute of Technology

In reference 1 Mehta suggested a method for extracting square roots of perfect square numbers by inspection. An article by King (reference 2) shows how to extract fifth roots from fifth powers of integers up to 150. We wish to present a different method of detecting square roots of perfect squares of numbers up to 1000. Of course, these methods work only if the given number is assured to be a square (or fifth power respectively). We first discuss some well-known properties of the decimal number system, after which we describe the algorithm.

When an integer is divided by 100, the remainder lies between 0 and 99. But which remainders can occur when only perfect squares are divided by 100? To answer this question we do not have to consider all the numbers $0^2, 1^2, 2^2, 3^2, \ldots$; we can, in fact, confine ourselves to the 26 numbers

$$0^2, 1^2, 2^2, \ldots, 25^2.$$

To prove this, we first note that

$$(50 + y)^2 - y^2 = 2500 + 100y, \tag{1}$$

so that $(50 + y)^2$ and y^2 have the same remainder; and secondly that

$$(50 - y)^2 - y^2 = 2500 - 100y, \tag{2}$$

so that $(50 - y)^2$ and y^2 have the same remainder. After examination of the integers $0^2, 1^2, \ldots, 25^2$, it is found that the possible remainders are the 21 numbers

$$0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41, 44, 49, 61, 64, 69, 76, 81, 84, 89, 96. \tag{3}$$

Now suppose that m is one of the numbers (3) other than 0 and 25. We are interested in the numbers x between 0 and 99 such that the division of x^2 by 100 leaves the remainder m. There are just four of these for each m, and they are of the form

$$y, 50 - y, 50 + y, 100 - y, \tag{4}$$

where y is a number in the range 1 to 24. The four numbers (4) are called the *candidates* for m; the number y in the range 1 to 24 is called *very minor*, $50 - y$ between 26 and 49 is called *fairly minor*, $50 + y$ between 51 and 74 is *fairly major* and $100 - y$ between 76 and 99 is *very major*.

† Address: 49 Hapudim St, Ramat Gan, Israel.

We shall see that it is not necessary to consider the remainder 0. For $m = 25$, there are ten candidates $x = 5, 15, 25, 35, 45, 55, 65, 75, 85, 95$. We notice however that, upon division by 1000, 5^2, 45^2, 55^2, 95^2 leave the remainder 25, while 15^2, 35^2, 65^2, 85^2 leave the remainder 225, and 25^2, 75^2 leave the remainder 625. In each group just one of the candidates is in each of the ranges 0 to 25, 25 to 50, 50 to 75, 75 to 100.

It is useful to tabulate the numbers from 1 to 25 which are not multiples of 10 with the remainders when their squares are divided by 100 (or by 1000 in the cases 5, 15, 25).

TABLE 1

y	y^2	y	y^2	y	y^2
01	01	09	81	18	24
02	04	11	21	19	61
03	09	12	44	21	41
04	16	13	69	22	84
05	025	14	96	23	29
06	36	15	225	24	76
07	49	16	56	25	625
08	64	17	89		

Next, by elementary algebra, for any z we have

$$(100z + 50)^2 = 10^4 z(z + 1) + 25 \cdot 10^2.$$

If z is a digit (0–9) we adopt decimal notation and write

$$100z + 50 = z50.$$

Then

$$\frac{1}{10^4}(z50)^2 = z(z + 1) + \frac{1}{10^2} \cdot 25. \tag{5}$$

Similar calculations yield the formulae

$$\frac{1}{10^4}(z25)^2 = \left(z(z + 1) - \frac{1}{2}z\right) + \frac{1}{10^4} \cdot 625 \tag{6}$$

$$\frac{1}{10^4}(z75)^2 = \left(z(z + 1) + \frac{1}{2}(z + 1)\right) + \frac{1}{10^4} \cdot 625. \tag{7}$$

These are all the prerequisites; we now describe the algorithm for finding $\sqrt{n}$, where n is known to be a perfect square and less than 1000^2. We shall proceed by means of examples, the first of which will be described in detail and some of the remaining ones a little more briefly. We first note that, if n is divisible by 10, then it is necessarily also divisible by 100; so we ignore this case since the problem then reduces to one for a number with fewer digits than n.

Example 1. $n = 12996$. We pair off the digits in the usual way prior to the extraction of a square root—1'29'96—and observe that the left-hand digit of the answer is $z = 1$. Also

$$\frac{n}{10^4} = 1{\cdot}2996 < z(z+1).$$

Hence, if the square root is $1pq$ (in decimal notation), it follows from (5) that pq is a minor candidate for 96. We still have to decide whether pq is very minor (i.e. 14) or fairly minor (i.e. 36). In fact,

$$\frac{n}{10^4} = 1{\cdot}2996 < z(z+1) - \frac{1}{2}z;$$

and it follows from (6) that pq is the very minor candidate 14 for 96. Therefore

$$\sqrt{n} = 114.$$

We continue to write $\sqrt{n} = zpq$ in the following examples.

Example 2. $n = 690561$. Now $z = 8$ and

$$\frac{n}{10^4} = 69{\cdot}0561 < 72 = z(z+1),$$

so that pq is a minor candidate for 61. But

$$z(z+1) - \tfrac{1}{2}z = 68$$

and therefore, by (6),

$$\frac{n}{10^4} > z(z+1) - \frac{1}{2}z + \frac{625}{10^4}.$$

Hence pq is the fairly minor candidate for 61, which is 31; and

$$\sqrt{n} = 831.$$

Example 3. $n = 228484$. Now $z = 4$ and

$$\frac{n}{10^4} = 22{\cdot}8484 > 22{\cdot}5625 = z(z+1) + \frac{1}{2}(z+1) + \frac{625}{10^4};$$

and so pq is the very major candidate for 84 and

$$\sqrt{n} = 478.$$

Example 4. $n = 50178$. Now $z = 2$ and

$$\frac{n}{10^4} < z(z+1) - \frac{1}{2}z + \frac{625}{10^4};$$

and so pq is the very minor candidate for 76, and

$$\sqrt{n} = 224.$$

Note that here the term 0·0625 determines the direction of the inequality, for

$$\frac{n}{10^4} > z(z+1) - \frac{1}{2}z.$$

In Examples 2 and 3 the difference between $n/10^4$ and the predominant term ($z(z+1) - \frac{1}{2}z$ and $z(z+1) + \frac{1}{2}(z+1)$ respectively) was much greater than 0·0625 and would have allowed us to ignore the latter term.

Example 5. $n = 265225$. Now $z = 5$ and

$$\frac{n}{10^4} < z(z+1) - \frac{1}{2}z;$$

and so pq is a very minor candidate for 25. If we take into account the last *three* digits of n we see that this candidate must be 15, and

$$\sqrt{n} = 515.$$

If Table 1 is memorised then, with a little practice, one ought to be able to perform the root extraction mentally. The announcement of the square root lends the performance a flavour of magic and should add fun to interest.

References

1. P. N. Mehta, Calculating square roots of perfect square numbers by inspection, *Math. Spectrum* **5** (1972/73), 46–48.
2. I. King, Extracting fifth roots a classroom activity, *Maths. Teacher* **67** (1974), 687–688.

More on Heronian Triangles

JOHN STRANGE
Goring Hall School, West Sussex

Formulae for Heronian triangles

A Heronian triangle is one whose sides and area are all integers. In Volume 8, Number 3, of *Mathematical Spectrum* Mr Sastry posed, and partially solved, the problem of determining all Heronian triangles. Starting from Hero's formula

$$\Delta = \sqrt{\{s(s-a)(s-b)(s-c)\}}$$

for the area Δ of a triangle with sides of length a, b, c and semi-perimeter s, and using an ingenious device to ensure that each of $s, s-a, s-b, s-c$ is a given multiple of a square, he proved that, if p, q, r, s are any integers and k is a positive integer, then the formula

$$\left.\begin{aligned} a &= 4k(p^2+q^2)(r^2+s^2) \\ b &= k[(p+r)^2+(q+s)^2][(p-r)^2+(q-s)^2] \\ c &= k[(p+s)^2+(q-r)^2][(p-s)^2+(q+r)^2] \end{aligned}\right\} \quad (1)$$

produces a Heronian triangle. However, we shall see that there exist Heronian triangles which cannot be obtained by Mr Sastry's method. For it will be proved that, if one side of a Heronian triangle contains a prime factor of the form $4h-1$, but $(4h-1)^2$ is not a factor, and if $4h-1$ is not a common factor of all three sides, then this triangle cannot be given by the formula (1).

In letters to the editor appearing in Volume 9, Number 2, Mr Tagg and Mr Pargeter gave further methods for producing Heronian triangles in which the guiding principle was to place side by side two right-angled triangles with integral sides. All formulae derived in this way involve an integral altitude (the common side of the right-angled triangles). But not all Heronian triangles can be obtained by this method; to prove this statement we shall exhibit a Heronian triangle having no integral altitude.

With the advent of 'modern' mathematics, some classical topics no longer receive the treatment they deserve. I fear that this may be true of the Euclidean algorithm. The simplicity and generality of this algorithm make it one of the finest mathematical achievements of all time. Here it will be sufficient to explain the procedure, and to illustrate it with an example; there is a full treatment of the algorithm on pp. 139–141 of reference 1. (The references are given at the end of the article.)

It may be shown that, given the positive integers n and d, there exists a unique non-negative integer q such that

$$qd \leqslant n < (q+1)d.$$

Writing $r = n - qd$, so that $0 \leqslant r < d$, we have

$$n = qd + r;$$

the number q is the quotient and r is the remainder in the division of n by d. We observe that any number which is a factor of both n and d is also a factor of r, while any number which is a factor of d and r is also a factor of n. So the problem of finding the common factors of n and d is equivalent to finding the common factors of d and r.

Suppose that we wish to find the G.C.D. (greatest common divisor) of 1219 and 901. We have

$$1219 = 1 \times 901 + 318,$$

so that we have only to find the G.C.D. of 901 and 318. Continuing in the same way we find that

$$\begin{aligned} 901 &= 2 \times 318 + 265, \\ 318 &= 1 \times 265 + 53, \\ 265 &= 5 \times 53. \end{aligned}$$

Since the G.C.D. of 265 and 53 is 53, it follows that the G.C.D. of 1219 and 901 is also 53.

Furthermore, working backwards, we have

$$\begin{aligned} 53 &= 318 - 265 \\ &= 318 - (901 - 2 \times 318) \\ &= 3 \times 318 - 901 \\ &= 3(1219 - 901) - 901 \\ &= 3 \times 1219 - 4 \times 901. \end{aligned}$$

It can, in fact, be proved quite generally that, if x and y are positive integers and if d is the G.C.D. of x and y, then there exist integers α and β such that

$$d = \alpha x + \beta y. \tag{2}$$

Now let a, b, c be the sides of a Heronian triangle ABC, let s be its semi-perimeter and let Δ be its area. Standard trigonometric formulae such as

$$\operatorname{tg} \frac{1}{2} B = \frac{\Delta}{s(s-b)}, \qquad \operatorname{tg} \frac{1}{2} C = \frac{\Delta}{s(s-c)}$$

show that $\operatorname{tg}\frac{1}{2}B$ and $\operatorname{tg}\frac{1}{2}C$ are rational, say m/n and p/q respectively (where m, n and p, q are coprime). Since

$$\cos\theta = \frac{1 - \operatorname{tg}^2\frac{1}{2}\theta}{1 + \operatorname{tg}^2\frac{1}{2}\theta}, \qquad \sin\theta = \frac{2\operatorname{tg}\frac{1}{2}\theta}{1 + \operatorname{tg}^2\frac{1}{2}\theta},$$

it follows that

$$\cos B = \frac{n^2 - m^2}{m^2 + n^2}, \qquad \sin B = \frac{2mn}{m^2 + n^2},$$

$$\cos C = \frac{q^2 - p^2}{p^2 + q^2}, \qquad \sin C = \frac{2pq}{p^2 + q^2}.$$

After a little algebra we therefore find that

$$\begin{aligned} \sin A = \sin(B + C) &= \sin B \cos C + \sin C \cos B \\ &= \frac{2(nq - mp)(mq + np)}{(m^2 + n^2)(p^2 + q^2)}. \end{aligned}$$

The sine formula then shows that

$$b = \frac{mn(p^2 + q^2)a}{(nq - mp)(mq + np)}, \qquad c = \frac{pq(m^2 + n^2)a}{(nq - mp)(mq + np)}. \tag{3}$$

Finally, from the formula $\Delta = \frac{1}{2}ca \sin B = \frac{1}{2}ab \sin C$ we get

$$\Delta(m^2 + n^2) = mnca, \qquad \Delta(p^2 + q^2) = pqab. \tag{4}$$

These equalities have several interesting consequences. Taking one of the relations (4), say the first, we see that any prime factor of $mnca$ of the form $4h - 1$ is a factor of Δ, because it is known that, when m and n are coprime, $m^2 + n^2$ has no such factors. (See reference 2, Theorem 367.)

Thus, for example, in the case of the 13, 14, 15 Heronian triangle, it follows from these considerations that the area is a multiple of 3 and 7. We are also able to assert, without calculation, that there is no Heronian triangle having the two sides 77, 103; for the area of such a triangle would have to be a multiple of 77 and 103, which is absurd since the area of a triangle is at most half the product of two of its sides.

Furthermore, it follows from the equality

$$(\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = (\alpha\gamma + \beta\delta)^2 + (\alpha\delta - \beta\gamma)^2$$

that each of the numbers a, b, c in Mr Sastry's formula (1) is a multiple of the sum of two squares. Now suppose that in a Heronian triangle one side has a prime factor $4h - 1$, but that $(4h - 1)^2$ is not a factor of that side and that $4h - 1$ does not divide both the other sides. If this triangle is given by a set of expressions of the form (1), then $4h - 1$ is not a factor of k, and so $4h - 1$ is a factor of the sum of two squares, say $x^2 + y^2$, while $(4h - 1)^2$ is not a factor of $x^2 + y^2$. However this is impossible since (according to Theorem 366 of reference 2) $x^2 + y^2$ cannot be divisible by the prime $4h - 1$ without also being divisible by $(4h - 1)^2$. Hence a Heronian triangle with these divisibility properties is not representable in the form (1). An example of such a triangle is 10, 35, 39, in which both 3 and 7 are prime factors of the required kind.

Returning again to the relations (4), let us suppose that $m^2 + n^2$ and $p^2 + q^2$ are coprime, i.e. that their G.C.D. is 1. Then, by (2), there exist integers α and β such that

$$\alpha(m^2 + n^2) + \beta(p^2 + q^2) = 1.$$

Hence

$$\alpha(m^2 + n^2)\,\Delta + \beta(p^2 + q^2)\,\Delta = \Delta,$$

so that, by (4),

$$(\alpha mnc + \beta pqb)a = \Delta.$$

This shows that a divides Δ and that the altitude corresponding to a is an (even) integer.

Heronian triangles without integral altitudes therefore have to be sought amongst those for which $m^2 + n^2$ and $p^2 + q^2$ are not coprime. The equality

$$(\alpha\gamma + \beta\delta)^2 + (\alpha\delta - \beta\gamma)^2 = (\alpha\delta + \beta\gamma)^2 + (\alpha\gamma - \beta\delta)^2$$

furnishes us with any number of pairs $(m, n), (p, q)$ for which $m^2 + n^2$ actually equals $p^2 + q^2$. For instance, $\alpha = 1, \beta = \gamma = 2, \delta = 3$ give $m = 4, n = 7, p = 1, q = 8$. By (3), the corresponding Heronian triangles are such that

$$b = \frac{35a}{39}, \qquad c = \frac{10a}{39}.$$

It is easily checked that none of the altitudes of the triangle whose sides are 39, 35, 10 is an integer. So we have here an example of a Heronian triangle which is not given by Mr Sastry's formulae, nor by those of Mr Pargeter and Mr Tagg.

In Mr Sastry's basic Heronian triangle ($k = 1$ in (1)) each of the numbers $s, s-a, s-b, s-c$ is a square (or twice a square). Since

$$s = (s-a) + (s-b) + (s-c),$$

integral solutions of

$$t^2 = x^2 + y^2 + z^2$$

are required. It is easily verified that one such solution is

$$t = 2\lambda^2 + \mu^2, \qquad x = 2\lambda\mu, \qquad y = 2\lambda^2, \qquad z = \mu^2$$

(where λ and μ are integers). This gives rise to the formulae

$$\begin{aligned} a &= t^2 - x^2 = \{\lambda^2 + (\lambda+\mu)^2\}\{\lambda^2 + (\lambda-\mu)^2\}, \\ b &= t^2 - y^2 = \mu^2(4\lambda^2 + \mu^2), \\ c &= t^2 - z^2 = 4\lambda^2(\lambda^2 + \mu^2) \end{aligned}$$

which make

$$\Delta = txyz = 4\lambda^3\mu^3(2\lambda^2 + \mu^2).$$

These formulae furnish further examples of Heronian triangles with no integral altitudes. One such triangle is obtained from $\lambda = 2$, $\mu = 1$; it is

$$a = 65, \qquad b = 17, \qquad c = 80, \qquad \Delta = 288.$$

Heronian triangles with consecutive integral sides

Having discovered the Heronian triangles 3, 4, 5 and 13, 14, 15, one is tempted to ask whether there are any more whose sides are consecutive integers.

Let $2x-1, 2x, 2x+1$ be the sides of such a triangle.† The area of this triangle is $\sqrt{(3x^2(x^2-1))}$, and so $\sqrt{(3(x^2-1))}$ has to be an integer. But, if $\sqrt{(3(x^2-1))}$ is an integer, then it is a multiple of 3. Hence we require solutions in non-negative integers of the equation

$$x^2 - 1 = 3y^2. \tag{5}$$

From (5) we deduce that $x^2 \geqslant 1$ and thus $x \geqslant 1$. We can therefore write $x = \mathrm{ch}(s)$, where s is a non-negative real number. Doing so we get

$$3y^2 = x^2 - 1 = \mathrm{ch}^2(s) - 1 = \mathrm{sh}^2(s),$$

so that $y = (1/\sqrt{3})\mathrm{sh}(s)$ (since y and $\mathrm{sh}(s)$ are both non-negative).

It is clear that $(x, y) = (1, 0)$ and $(x, y) = (2, 1)$ are integral solutions of (5). These solutions correspond to $s = 0$ and $s = \alpha$ respectively, where $\mathrm{sh}(\alpha) = \sqrt{3}$, i.e. $\alpha = \arg\mathrm{sh}(\sqrt{3})$. As $(1/\sqrt{3})\mathrm{sh}$ increases from 0 at 0 to 1 at α, and as there is no integer strictly between 0 and 1, α is the least (strictly) positive parameter giving a solution of (5).

† We need not consider triangles of the type $2x, 2x+1, 2x+2$, since their semi-perimeters are not integers and they are consequently not Heronian.

Let s and t be parameters of solutions. We show that $s + t$ is also the parameter of a solution. Since

$$(x, y) = \left(\mathrm{ch}(s + t), \frac{1}{\sqrt{3}}\,\mathrm{sh}(s + t)\right)$$

satisfies (5), it is only necessary to verify that $\mathrm{ch}(s + t)$ and $(1/\sqrt{3})\mathrm{sh}(s + t)$ are non-negative integers. But this follows from the identities

$$\mathrm{ch}(s + t) = \mathrm{ch}(s)\mathrm{ch}(t) + 3\left(\frac{1}{\sqrt{3}}\,\mathrm{sh}(s)\right)\left(\frac{1}{\sqrt{3}}\,\mathrm{sh}(t)\right),$$

$$\frac{1}{\sqrt{3}}\,\mathrm{sh}(s + t) = \left(\frac{1}{\sqrt{3}}\,\mathrm{sh}(s)\right)\mathrm{ch}(t) + \mathrm{ch}(s)\left(\frac{1}{\sqrt{3}}\,\mathrm{sh}(t)\right)$$

and from the hypothesis that s, t are parameters of integral solutions. It is proved in the same way that $s - t$ is the parameter of a solution if $s \geqslant t$.

Next we note that, if n is a non-negative integer, then $n\alpha$ is the parameter of a solution (where α was defined as the least positive parameter of a solution). Now let β be the parameter of a solution. Let n be the integer such that

$$n\alpha \leqslant \beta < (n + 1)\alpha$$

and therefore

$$0 \leqslant \beta - n\alpha < \alpha. \tag{6}$$

(It can be proved that such an integer exists and is unique.) From the previous paragraph we know that $\beta - n\alpha$ is the parameter of a solution; and, since no parameter of a solution lies strictly between 0 and α, (6) shows that $\beta - n\alpha = 0$. Thus every parameter of a solution is of the form $n\alpha$, where n is a non-negative integer.

The required solutions of (5) are thus all the couples of the form

$$(x_n, y_n) = \left(\mathrm{ch}(n\alpha), \frac{1}{\sqrt{3}}\,\mathrm{sh}(n\alpha)\right),$$

where n is a non-negative integer. This means that all the Heronian triangles whose sides are consecutive integers are given by

$$2\mathrm{ch}(n\alpha) - 1, \qquad 2\mathrm{ch}(n\alpha), \qquad 2\mathrm{ch}(n\alpha) + 1 \quad (n = 0, 1, 2, \ldots).$$

The area of the triangle with parameter $n\alpha$ is $\sqrt{3}\mathrm{ch}(n\alpha)\mathrm{sh}(n\alpha) = \frac{1}{2}\sqrt{3}\mathrm{sh}(2n\alpha)$.

For every non-negative integer n, let

$$\boldsymbol{u}_n = (x_n, y_n) = \left(\mathrm{ch}(n\alpha), \frac{1}{\sqrt{3}}\,\mathrm{sh}(n\alpha)\right).$$

Then

$$\begin{aligned}\boldsymbol{u}_{n+k} + \boldsymbol{u}_{n-k} &= \left(2\mathrm{ch}(n\alpha)\mathrm{ch}(k\alpha), \frac{2}{\sqrt{3}}\,\mathrm{sh}(n\alpha)\mathrm{ch}(k\alpha)\right) \\ &= 2\mathrm{ch}(k\alpha)\boldsymbol{u}_n. \end{aligned} \tag{7}$$

In particular, since $\mathrm{ch}(\alpha) = 2$,

$$u_{n+1} = 4u_n - u_{n-1};$$

and from this recurrence formula we easily calculate the first few terms of the sequence (u_n). They are

$$(1, 0), (2, 1), (7, 4), (26, 15), (97, 56), (362, 209),$$
$$(1351, 780), (5042, 2911), (18817, 10864), \ldots.$$

To obtain u_{42}, for example, we might proceed as follows. First, putting $n = k = 1$ in (7), we get $u_2 = (7, 4)$. Next, with $k = 2$ we take $n = 2$, so that

$$u_4 + u_0 = 2\mathrm{ch}(2\alpha)u_2$$

and

$$u_4 = 14u_2 - u_0 = (97, 56).$$

Then $k = 2$ and $n = 4$ give

$$u_6 + u_2 = 2\mathrm{ch}(2\alpha)u_4,$$

whence

$$u_6 = 14u_4 - u_2 = (1351, 780).$$

Finally, with $k = 6$, we take n to be 6, 12, 18, 24, 36 in turn. In this way we successively obtain $u_{12}, u_{18}, \ldots, u_{42}$.

Alternatively, taking $n = k = 1$, then $n = k = 2$, $n = k = 4$, $n = k = 8$, $n = k = 16$ in (7) we can calculate $u_2, u_4, u_8, u_{16}, u_{32}$. The formulae for $\mathrm{ch}(s + t)$ and $\mathrm{sh}(s + t)$ with $s = 32\alpha$ and $t = 8\alpha$ now give u_{40}. Finally, using the same formulae with $s = 40\alpha$ and $t = 2\alpha$ we get u_{42}.

A word of warning to those who may wish to try: x_{42} and y_{42} are 24-digit numbers!

The sequences $(x_n), (y_n)$ have some interesting arithmetical properties. For example, the following results hold (but their proofs are too difficult for inclusion):

(i) If p is a prime greater than 2, then $x_p - 2 = \mathrm{ch}(p\alpha) - 2$ is a multiple of p.

(ii) If p is a prime of the form $12n \pm 5$, then $y_p + 1 = (1/\sqrt{3})\mathrm{sh}(p\alpha) + 1$ is a multiple of p; and if p is a prime of the form $12n \pm 1$, then $y_p - 1 = (1/\sqrt{3}) \times \mathrm{sh}(p\alpha) - 1$ is a multiple of p.

The rest of this article is devoted to other properties of (x_n) and (y_n) which are more easily proved.

When x, y, α, β are integers, then $\alpha x + \beta y$ is clearly a multiple of the G.C.D. of x and y. If, therefore, $\alpha x + \beta y = 1$, then the G.C.D. of x and y is 1, i.e. x and y are coprime. The equalities

$$x_n y_{n+1} - x_{n+1} y_n = \frac{1}{\sqrt{3}} \mathrm{sh}((n + 1)\alpha - n\alpha) = \frac{1}{\sqrt{3}} \mathrm{sh}(\alpha) = 1$$

consequently show that x_n and y_n, x_n and x_{n+1}, y_n and y_{n+1} are pairs of coprime integers.

It is easily proved that y_{mn} is a multiple of y_n. For

$$\mathrm{sh}((m+1)n\alpha) = \mathrm{ch}(n\alpha)\mathrm{sh}(mn\alpha) + \mathrm{ch}(mn\alpha)\mathrm{sh}(n\alpha),$$

so that, on dividing by $\sqrt{3}$, we have

$$y_{(m+1)n} = x_n y_{mn} + x_{mn} y_n.$$

Thus, if y_{mn} is a multiple of y_n, so also is $y_{(m+1)n}$. Since $y_0 = 0$ is a multiple of y_n, the result follows at once by induction on m.

We can now prove that the G.C.D. of y_m and y_n is y_d, where d is the G.C.D. of m and n.

In the first place it is useful to define x_n and y_n also for negative n. Since $\mathrm{ch}(-s) = \mathrm{ch}(s)$ and $\mathrm{sh}(-s) = -\mathrm{sh}(s)$, we put $x_{-n} = x_n$ and $y_{-n} = -y_n$. Next we note that, by (2), there exist integers λ and μ (one of which is negative) such that

$$d = \lambda m + \mu n.$$

Hence, by the formula for $\mathrm{sh}(s+t)$,

$$y_d = y_{\lambda m + \mu n} = x_{\mu n} y_{\lambda m} + x_{\lambda m} y_{\mu n}.$$

This shows that any number dividing $y_{\lambda m}$ and $y_{\mu n}$ also divides y_d; and since y_m divides $y_{\lambda m}$ and y_n divides $y_{\mu n}$, any common factor of y_m and y_n is also a factor of y_d. On the other hand, since d divides m and n, y_d divides y_m and y_n. This completes the proof.

As y_m and y_n both divide y_{mn}, $y_m y_n$ divides $y_{mn} y_d$. In particular, if m and n are coprime, then $y_m y_n$ divides y_{mn}.

The sequence (x_{2^n}), i.e. $(\mathrm{ch}(2^n\alpha))$, is of interest as E. Lucas showed that, if p is a prime greater than 2, then $2^p - 1$ is prime if and only if it divides $\mathrm{ch}(2^{p-2}\alpha)$. Using this result he was able to prove that $2^{127} - 1$ is prime, and this number was the largest known prime from 1876 until 1952.†

It is a little more convenient to consider the sequence (v_n), where

$$v_n = 2\mathrm{ch}(2^n\alpha) \quad (n = 0, 1, 2, \ldots)$$

(rather than $\mathrm{ch}(2^n\alpha)$). This sequence can be defined recursively by

$$v_0 = 4, \quad v_{n+1} = v_n^2 - 2 \quad (n = 0, 1, 2, \ldots);$$

that this is so follows from the identity

$$2\mathrm{ch}(2s) = (2\mathrm{ch}(s))^2 - 2.$$

† It is now known that $2^{11213} - 1$ is a prime. This fact was established in 1963 in the University of Illinois with the help of the university's computer. The Mathematics Department's franking machine proudly proclaimed the message, and the first issue of *Mathematical Spectrum* contained an article on computing in which the stamp was reproduced.

The first four terms of the sequence $(v_n - 1)$, namely

$$3, 13, 193, 37633$$

are prime, and it has been demonstrated by use of a computer that the fifth term,

$$1416\,317953,$$

is also a prime. However

$$2\,005956\,546822\,746113,$$

the next member of the sequence, is not prime since 769 is a factor. The search for this factor was laborious, but not to such an extent as might first be expected. For I have proved that (if $n \neq 0$) every factor of $v_n - 1$ is of the form $12m + 1$; the factor 769 was then found by making a list of primes of this form and trying each in turn. To test $v_n - 1$ for divisibility by a prime p we express v_n modulo p by making use of the recurrence relation $v_{k+1} = v_k^2 - 2$. For instance, when $p = 769$, we have

$$v_0 \equiv 4, \quad v_1 \equiv 16 - 2 \equiv 14, \quad v_2 \equiv 196 - 2 \equiv 194,$$
$$v_3 \equiv 37636 - 2 \equiv 37634 \equiv -47, \quad v_4 \equiv 2209 - 2 \equiv 2207 \equiv -100,$$
$$v_5 \equiv 10000 - 2 \equiv 9998 \equiv 1.$$

Thus $v_5 - 1$ is divisible by 769. In other cases we may be able to establish even more than we set out to prove. If $p = 757$,

$$v_0 \equiv 4, \quad v_1 \equiv 14, \quad v_2 \equiv 194, \quad v_3 \equiv 37636 - 2 \equiv -216,$$
$$v_4 \equiv 46656 - 2 \equiv -280, \quad v_5 \equiv 78400 - 2 \equiv -330,$$
$$v_6 \equiv 108900 - 2 \equiv -110, \quad v_7 \equiv 12100 - 2 \equiv -14.$$

Since $(-14)^2 = 14^2$, it is now clear that $v_n + 6 \equiv v_n$ for all $n \geqslant 2$. But $v_0, \ldots, v_7$ are not equivalent to 1 modulo 757, and so none of the v_n is equivalent to 1 modulo 757. It follows that 757 is not a factor of any of the $v_n - 1$.

The recurrence relation defining (v_n) can be written

$$v_{n+1} + 1 = (v_n + 1)(v_n - 1)$$

and from this it follows by induction on k that

$$v_{n+k} + 1 = (v_n + 1)(v_n - 1)(v_{n+1} - 1) \cdots (v_{n+k-1} - 1). \tag{8}$$

We use this equality and the Euclidean algorithm to find the G.C.D. of $v_n - 1$ and $v_{n+k} - 1$ $(k \geqslant 1)$. By (8), $v_n - 1$ divides $v_{n+k} + 1$, i.e.

$$v_{n+k} + 1 = m(v_n - 1),$$

say. Hence $v_{n+k} - 1 = m(v_n - 1) - 2$, or

$$v_{n+k} - 1 = p(v_n - 1) + (v_n - 3), \tag{9}$$

where $p = m - 1$. Also

$$v_n - 1 = 1(v_n - 3) + 2 \tag{10}$$

and, since v_n is even,

$$v_n - 3 = q^2 + 1. \tag{11}$$

The successive divisions (9), (10), (11) constitute the steps of Euclid's algorithm for calculating the G.C.D. of $v_{n+k} - 1$ and $v_n - 1$. This G.C.D. is therefore 1 (the remainder in (11)), which means that any two distinct terms of the sequence $(v_n - 1)$ are coprime.

Furthermore, each term of the sequence $(v_n - 1)$ (except the first, $v_0 - 1$) is the sum of two squares. This follows from the formula

$$\mathrm{ch}^2(2^{n-1}\alpha) + 3\mathrm{sh}^2(2^{n-1}\alpha) = 2\mathrm{ch}(2^n\alpha) - 1,$$

which is easily verified. Thus

$$13 = 2^2 + 3^2, \quad 193 = 7^2 + 12^2, \quad 37633 = 97^2 + 168^2,$$
$$1416\,317953 = 18817^2 + 32592^2, \ldots . \tag{12}$$

Since $v_0 = 4$, $v_0 + 1 = 5 = 1^2 + 2^2$. Then, from (8) with $n = 0$ and from (12) we deduce that $v_1 + 1, v_2 + 1, v_3 + 1, \ldots$ are

$$3(1^2 + 2^2), 3(1^2 + 2^2)(2^2 + 3^2), 3(1^2 + 2^2)(2^2 + 3^2)(7^2 + 12^2), \ldots,$$

respectively.

We defined v_n to be $2x_{2^n} = 2\mathrm{ch}(2^n\alpha)$. The members of the sequence (y_{2^n}), i.e. $((1/\sqrt{3})\mathrm{sh}(2^n\alpha))$ can be expressed in terms of $v_0, v_1, v_2, \ldots$; in fact, it is easily proved by induction on n that

$$y_{2^n} = v_0 v_1 \ldots v_{n-1}.$$

Finally, here are two Heronian problems awaiting solution: Given a natural number n, determine

(i) every Heronian triangle whose semi-perimeter is n,
(ii) every Heronian triangle whose area is n.

References

1. Hazel Perfect, *Topics in Algebra* (Pergamon Press, Oxford, 1966).
2. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edition (Clarendon Press, Oxford, 1960).

Letters to the Editor

Dear Editor,

The general quartic

By solving a geometrical puzzle, I was led to an easy method for calculating a reducing cubic of a quartic equation; I think it is more direct than Ferrari's method. Here I will first give the general solution and then the puzzle as an example.

By division of the leading coefficient, a quartic (in common with any polynomial equation) can be reduced to 'monic' form:

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

If this is written in factorized form as

$$(x^2 + kx + l)(x^2 + mx + n) = 0$$

then, upon equating coefficients, we have

$$k + m = a \quad (1) \qquad km + l + n = b \quad (2)$$
$$kn + lm = c \quad (3) \qquad ln = d \quad (4)$$

and therefore, if $l + n = 2\lambda$, we obtain from (1), (2), (4) the values

$$a/2 \pm \sqrt{[(\tfrac{1}{4}a^2 - b) + 2\lambda]}$$

for k and m, and the values

$$\lambda \pm \sqrt{(\lambda^2 - d)}$$

for l and n. Substitution in (3) gives

$$c = a\lambda \pm 2\sqrt{[(\lambda^2 - d)((\tfrac{1}{4}a^2 - b) + 2\lambda)]}$$

or equivalently,

$$(\lambda^2 - d)(8\lambda + (a^2 - 4b)) = (a\lambda - c)^2;$$

which is a cubic in λ.

There are, in general, three distinct ways of resolving a quartic into quadratic factors; these will be obtained from the three possible values of λ. If the cubic does not have an integer root, the roots of the original quartic may be too awkward for any practical purposes.

As an example, let us evaluate u, v in the following construction:

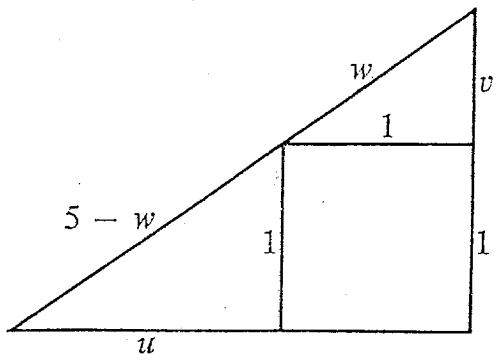


Figure 1

We have $u^2 = (5 - w)^2 - 1^2$, $v^2 = w^2 - 1^2$ and, upon equating two expressions for area, also

$$1^2 + \tfrac{1}{2}u + \tfrac{1}{2}v = \tfrac{1}{2}[(1 + u)(1 + v)].$$

Therefore

$$u^2v^2 = 1;$$

and hence

$$((5 - w)^2 - 1)(w^2 - 1) = 1,$$

i.e.

$$w^4 - 10w^3 + 23w^2 + 10w - 25 = 0. \qquad (5)$$

After some simplification, the reducing cubic is

$$2(\lambda^2 + 25)(\lambda + 1) = 25(\lambda + 1),$$

which has an obvious root $\lambda = -1$. Consequently $k = m = -5$, $l = -1 + \sqrt{26}$, $n = -1 - \sqrt{26}$ (say); and the quartic equation (5) becomes

$$(w^2 - 5w - (1 - \sqrt{26}))(w^2 - 5w - (1 + \sqrt{26})) = 0$$

with roots

$$\tfrac{1}{2}(5 \pm \sqrt{[29 - 4\sqrt{26}]}), \quad \tfrac{1}{2}(5 \pm \sqrt{[29 + 4\sqrt{26}]}).$$

In view of the construction, $1 < 5 - w$ and $1 < w$; i.e. $1 < w < 4$; and therefore

$$w = \tfrac{1}{2}(5 \pm \sqrt{[29 - 4\sqrt{26}]}).$$

Finally, the values of u, v (in either order) are

$$\tfrac{1}{2}\sqrt{[(5 \pm \sqrt{(29 - 4\sqrt{26})})^2 - 4]}.$$

Yours sincerely,
JOHN R. RAMSDEN
(University of Aston, Birmingham)

Dear Editor,

The area of a polygon

Many readers who have at one time or another drawn a polygon on squared paper must have asked themselves how its area was related to the number of lattice points it enclosed. If we are given a polygon and are allowed to choose the grid, then the number of lattice points enclosed is a good approximation to the area (as defined by the grid) provided that the squares are sufficiently small. On the other hand, when the grid is fixed the situation is much less simple, since we can, for instance, draw long but thin rectangles of large area which do not contain any lattice points at all. However, a colleague, Mr Alan Asbury, who considered the problem, obtained an exact formula applicable to polygons whose vertices lie on lattice points. Although Mr Asbury had, in fact, been anticipated as long ago as 1899 by G. Pick, the result is not too well known; and it is so remarkable that I feel sure its publication in *Mathematical Spectrum* will be welcomed. So here are the theorem and its proof.

Theorem. If a polygon has its vertices on lattice points, then its area is

$$i + \tfrac{1}{2}s - 1,$$

where i is the number of lattice points in the interior of the polygon and s is the number of lattice points through which the sides pass (including the vertices themselves).

Proof. (i) We begin by considering two polygons P and Q, all of whose vertices lie on lattice points, where Q is obtained from P by the addition of a triangle Δ. Suppose that the common side of P and Δ contains h lattice points, excluding the end points, and that the other two sides of Δ contain k and l lattice points, again excluding the end points. Denoting by s_P and i_P the numbers of lattice points on the sides and in the interior of P, respectively, and using an analogous notation for Δ and Q, we have

$$\begin{aligned} i_Q + \tfrac{1}{2}s_Q - 1 &= (i_P + i_\Delta + h) + \tfrac{1}{2}(s_P - h + k + l + 1) - 1 \\ &= (i_P + \tfrac{1}{2}s_P - 1) + i_\Delta + \tfrac{1}{2}(h + k + l + 3) - 1 \\ &= (i_P + \tfrac{1}{2}s_P - 1) + (i_\Delta + \tfrac{1}{2}s_\Delta - 1). \end{aligned}$$

Therefore if the formula for the area applies to P and Δ, then it also applies to Q. Since any polygon can be made up from triangles whose vertices are also vertices of the polygon, it is sufficient to prove the formula for a triangle.

(ii) Let ABC be a triangle whose vertices lie on lattice points and suppose that A is the vertex (or one of the vertices) with least x-coordinate. The origin may be taken to be at A; let B, C have coordinates (m, n), (p, q), respectively. Then $m, p \geqslant 0$ and, if also $m \geqslant p \geqslant 0$ and $q \geqslant n \geqslant 0$, we obtain a diagram such as the one in the figure (with some simplification

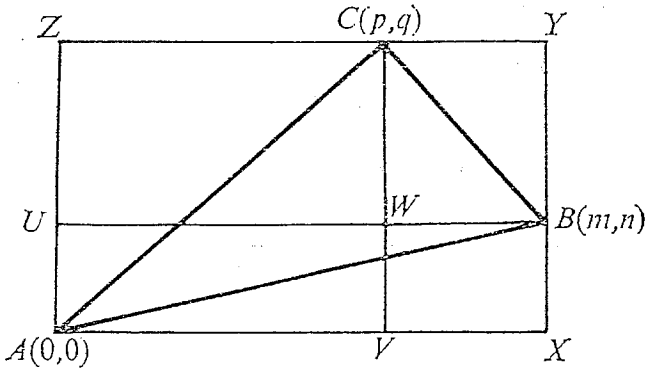


Figure 1

when one of n, p is 0 or $m = p$ or $n = q$). We may confine our attention to triangles of this kind, for other triangles can be obtained from this basic type by reflection in an axis or by composition.

In the notation corresponding to that used in (i),

$$i_{AXYZ} = i_{ABC} + i_{AXB} + i_{BYC} + i_{CZA} + a + b + c, \qquad (*)$$

where a, b, c are the numbers of lattice points, other than A, B, C, on the sides BC, CA, AB, respectively. Now

$$\begin{aligned} i_{AXYZ} &= (m-1)(q-1), \\ i_{AXB} &= \tfrac{1}{2}(i_{AXBU} - c) = \tfrac{1}{2}\{(m-1)(n-1) - c\}, \\ i_{BYC} &= \tfrac{1}{2}(i_{BYCW} - a) = \tfrac{1}{2}\{(m-p-1)(q-n-1) - a\}, \\ i_{CZA} &= \tfrac{1}{2}(i_{CZAV} - b) = \tfrac{1}{2}\{(p-1)(q-1) - b\}. \end{aligned}$$

It therefore follows from (*) (after a certain amount of algebra) that

$$i_{ABC} = \tfrac{1}{2}mq - \tfrac{1}{2}np - \tfrac{1}{2} - \tfrac{1}{2}(a + b + c).$$

Also

$$s_{ABC} = a + b + c + 3$$

and so

$$i_{ABC} + \tfrac{1}{2}s_{ABC} - 1 = \tfrac{1}{2}mq - \tfrac{1}{2}np.$$

But it is easily seen from the figure that the area of ABC is

$$mq - \tfrac{1}{2}mn - \tfrac{1}{2}(m-p)(q-n) - \tfrac{1}{2}pq = \tfrac{1}{2}mq - \tfrac{1}{2}np.$$

Thus the required expression for the area holds in the case of the triangle ABC, and the proof of the theorem is complete.

Yours sincerely,

G. F. A. HOFFMANN DE VISME
(North Staffordshire Polytechnic, Beaconside, Stafford)

Dear Editor,

Proportions of identical and fraternal twins

Lindley (reference 1, Part 1, pp. 21–22) gives the following example as an illustration of the use of the generalized addition law of probability.

In the sample space of observed sets of human twins let there be a pairs in which both twins are male, b pairs of mixed sex, and c pairs in which both are female. Each pair of twins will either be identical (event A) or fraternal (event $\bar{A}$). For a given pair of twins of the same sex it is difficult to determine the probability of their being identical. But if we suppose that (i) at each birth of twins there is a probability $p(A)$ that they are identical, and (ii) at each birth males and females are equally likely and that the two members of a pair of fraternal twins have independent determinations of sex, then the probability of two twins being male is

$$p(MM) = p(MM|A)p(A) + p(MM|\bar{A})p(\bar{A}) = \tfrac{1}{2}p(A) + \tfrac{1}{4}(1 - p(A)).$$

From this we get

$$p(A) = 4p(MM) - 1,$$

which can be estimated by

$$p(A) = \frac{4a}{a+b+c} - 1 = \frac{3a-b-c}{a+b+c},$$

since a, b and c are readily determined by observation.

There are two objections that can be raised to this procedure. Firstly, a similar argument can be used to get the estimate

$$p(A) = 4p(FF) - 1 = \frac{-a-b+3c}{a+b+c}$$

which, for reasons of symmetry, should be just as reliable as the previous one, although it will not be equal to it unless $a = c$. Secondly, the estimator can yield absurd values for $p(A)$. For instance, if $a = 1$, $b = 3$ and $c = 4$ it gives

$$p(A) = \frac{3a-b-c}{a+b+c} = -\frac{1}{2}$$

(which could, presumably, be 'rounded up' to a feasible value $p(A) = 0$); and if $a = 5$, $b = 1$, $c = 2$ it gives $p(A) = \frac{8}{2}$ which, on rounding down to $p(A) = 1$, is still absurd because it would be impossible to get the pair of twins of mixed sexes if all twin births were identical twins.

There is also the possibility of estimating $p(A)$ by considering

$$p(MF) = p(MF|A)p(A) + p(MF|\bar{A})p(\bar{A}) = 0 \,.\, p(A) + \tfrac{1}{2}(1 - p(A)).$$

This leads to

$$p(A) = 1 - 2p(MF) = \frac{a-b+c}{a+b+c},$$

which is seen to be the arithmetic mean of the other two estimators, and might therefore be expected to be superior to either of them. To verify that this is the case, let x be the value of $p(A)$. Then, in n pairs of twins, the expected numbers of male, female and mixed pairs are

$$\begin{aligned} E(MM) &= E(\text{no. of identical pairs})\, p(MM|A) \\ &\quad + E(\text{no. of fraternal pairs})\, p(MM|\bar{A}) \\ &= nx \,.\, \tfrac{1}{2} + (n - nx) \,.\, \tfrac{1}{4} = n(1 + x)/4, \\ E(FF) &= n(1 + x)/4, \\ E(MF) &= nx \,.\, 0 + (n - nx) \,.\, \tfrac{1}{2} = n(1 - x)/2. \end{aligned}$$

For a least squares estimate of x we must minimize the sum $S = \Sigma$ (observed frequency − expected frequency)^2, where the summation is taken over all the possible classes of outcomes *MM*, *FF* and *MF*. Thus

$$S = \{n(1 + x)/4 - a\}^2 + \{n(1 + x)/4 - c\}^2 + \{n(1 - x)/2 - b\}^2,$$

where $n = a + b + c$. Differentiation and simplification leads to

$$0 = \frac{dS}{dx} = \frac{n}{4}(3nx - n - 2a + 4b - 2c),$$

whence

$$x = \frac{n + 2a - 4b + 2c}{3n} = \frac{a - b + c}{a + b + c}.$$

Since S was a quadratic in x with the coefficient of x^2 greater than zero, it follows that S has a relative minimum and so the least squares estimate of $p(A)$ is $(a - b + c)/(a + b + c)$. Unlike the other estimators considered, this function cannot exceed 1; but it can be negative, when $b > a + c$, in which case it is easily seen from the graph of a quadratic S with a minimum turning point in the halfplane $x < 0$ that the least value of S, subject to the constraint $x \geq 0$, is attained at $x = 0$. There is no theoretical objection to estimating $p(A)$ to be 0 when the number of pairs of twins of opposite sex is large, and so the final estimator of $p(A)$ can be expressed as

$$\hat{p}(A) = \max\left(0, \frac{a - b + c}{a + b + c}\right).$$

Yours sincerely,
A. V. Boyd
(University of the Witwatersrand, Johannesburg)

Dear Editor,

Calculation of π to 99 decimal places

In 1671 James Gregory (1638–1675) discovered the simple formula

$$\pi = 4 \arctan 1 = 4\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots\right).$$

However, this is impractical for the calculation of π as, for example, about 10^7 terms of the series are required to obtain a value correct to 7 decimal places. On the other hand, the power series in the identity

$$\arctan x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots \quad (-1 \leqslant x \leqslant 1) \tag{1}$$

converges quite rapidly for relatively small values of x and this fact can be used to obtain good approximations to π.

It is easily proved that

$$\arctan x + \arctan y = \arctan\left(\frac{x + y}{1 - xy}\right) \quad (xy < 1). \tag{2}$$

Applying this formula twice we have

$$2 \arctan \frac{1}{5} = \arctan \frac{5}{12} \quad \text{and} \quad 2 \arctan \frac{5}{12} = \arctan \frac{120}{119},$$

so that

$$\arctan \frac{120}{119} = 4 \arctan \frac{1}{5}. \tag{3}$$

Now take $x = 120/119$. Then $(x + y)/(1 - xy) = 1$ if $y = -1/239$. Since arc tan $(-y) =$ $-$arc tan y, it follows from (2) and (3) that

$$4 \arctan \frac{1}{5} - \arctan \frac{1}{239} = \arctan 1 = \frac{1}{4}\pi,$$

i.e.

$$\pi = 16 \arctan \frac{1}{5} - 4 \arctan \frac{1}{239}. \tag{4}$$

This identity was discovered in 1706 by John Machin (1680–1751).

To calculate π we use (4) and (1). For instance, a value correct to 7 decimal places is obtained from the first seven terms of the series for arc tan $\frac{1}{5}$ and just the first term of the series for arc tan 1/239. Really great accuracy can obviously be achieved with a computer.

Using multiple precision arithmetic procedures developed by Hill (reference 1) I have written an Algol 60 program to compute π from (4) and (1) to 99 decimal places on the ICL 1905F at Lancaster University. This computer has a cycle time of 650 nanoseconds and evaluation was achieved in an execution time of 538 seconds. The result obtained,

$$\begin{array}{lllllllll} \pi \simeq 3{\cdot}141 & 592 & 653 & 589 & 793 & 238 & 462 & 643 & 383 \\ 279 & 502 & 884 & 197 & 169 & 399 & 375 & 105 & 820 \\ 974 & 944 & 592 & 307 & 816 & 406 & 286 & 208 & 998 \\ 628 & 034 & 825 & 342 & 117 & 068 & & & \end{array}$$

corresponds, correctly rounded, to the first 99 places in the value of π to 100,000 decimal places computed by Shanks and Wrench (reference 2). Seventy-two iterations were required to compute arc tan $\frac{1}{5}$ and 21 iterations for arc tan 1/239.

References

1. I. D. Hill, Procedures for the basic arithmetical operations in multiple-length working, *The Computer Journal* **11** (1968), 232–235.

2. D. Shanks and J. W. Wrench, Jr, Calculation of π to 100,000 decimals, *Math. Comp.* **16** (1962), 76–99.

Yours sincerely,

JOHN S. HAMPTON
(63 Cork Road, Lancaster)

Dear Editor,

Euler's formulae for rational Heronian triangles

May I comment on the interesting article on Heronian triangles by K. R. S. Sastry in Vol. 8, No. 3? In fact, formulae for Heronian triangles were derived by Euler (*Opera postuma* **1**, 1862), but (according to L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, 1920) the details of his proof have been lost. So it may be worthwhile outlining a proof of the formulae.

We shall refer to a triangle ABC with rational sides and area as a rational Heronian triangle. Let AL be the perpendicular from A to BC. Since $a \cdot AL = 2\Delta$, AL is rational; and, by the cosine formula, the cosines of the angles of the triangle are rational. It then follows that BL/c and LC/b are rational. Hence the triangles ALB, ALC are rational Pythagorean triangles. Thus every rational Heronian triangle can be constructed by juxtaposing two Pythagorean triangles. When subdividing a rational Heronian triangle into two Pythagorean ones we may clearly choose an internal altitude. Sastry has given the formulae for the sides of a Pythagorean triangle as $(m^2 - n^2)q$, $2mnq$, $(m^2 + n^2)q$ and to obtain the rational triangles we may assume m, n integral and q rational. Note that this triangle also arises as $2m_1n_1q_1$, $(m_1^2 - n_1^2)q_1$, $(m_1^2 + n_1^2)q_1$, where $m_1 = m + n$, $n_1 = m - n$ and $q_1 = q/2$. Therefore in juxtaposing two such triangles we can arrange them so that the sides of the form $2mnq$ coincide and form an altitude of the new triangle.

Euler gives the formula for rational Heronian triangles with sides a, b, c as

$$a : b : c = \frac{(ps \pm qr)(pr \mp qs)}{pqrs} : \frac{p^2 + q^2}{pq} : \frac{r^2 + s^2}{rs}.$$

We obtain this formula by taking triangles $(p^2 - q^2)\lambda$, $2pq\lambda$, $(p^2 + q^2)\lambda$ and $(r^2 - s^2)\mu$, $2rs\mu$, $(r^2 + s^2)\mu$ with $2pq\lambda = 2rs\mu$, and juxtaposing them. The resulting triangle has sides $a = (p^2 - q^2)\lambda + (r^2 - s^2)\lambda pq/rs$, $b = (p^2 + q^2)\lambda$, $c = (r^2 + s^2)\lambda pq/rs$. Dividing by λpq and simplifying gives the result with the top signs. We are assuming p, q, r, s integers with $p > q$, $r \geqslant s$. The formula with the bottom signs arises when the common altitude is taken to be external rather than internal. This is equivalent to interchanging r and s. We include the case $r = s$ to give the Pythagorean triangles.

It should be noted that integral Heronian triangles do not necessarily give rise to integral Pythagorean triangles. For example, the triangle with sides 10, 35, 39 has area 168; thus none of its altitudes is integral, and so it arises from rational, but not integral, Pythagorean triangles.

The formulae given by Sastry† give rise only to Heronian triangles in which the ratios $a + b + c : a + b - c : a - b + c : -a + b + c$ are squares of rational numbers. This need not be the case for general Heronian triangles as the above example shows.

Yours sincerely,
A. D. SANDS
(University of Dundee)

† These formulae are restated on p. 15, at the beginning of the article by John Strange.

Problems and Solutions

Sixth formers and students are invited to submit solutions to some or all of the problems below: the most attractive solutions will be published in subsequent issues. When writing to the Editorial Office, please state your full name and the postal address of your school, college or university.

10.1. (Submitted by B. G. Eke, University of Sheffield.) Show that the sum of the lengths of the diagonals of a plane quadrilateral exceeds the sum of the lengths of two opposite sides.

10.2. A pyramid on a triangular base has the length of each sloping side one unit and the length of each base side $\sqrt{2}$ units. The point P is a point of the base, distant d_1, d_2, d_3 units from the base vertices. Determine the distance of P from the apex of the pyramid.

10.3. (Submitted by T. B. Cruddis, University of Sheffield.) The real numbers p, q, r are such that $q \neq r$ and $2p = q + r$. Show that

$$\frac{p^{q+r}}{q^q r^r} < 1.$$

Solutions to Problems in Volume 9, Number 2

9.4. What is the expression in base 7 of the square root of the number whose expression in base 7 is 14,641?

Solution by Alan Burns (W. R. Tuson College, Preston)

$$\begin{aligned}(14,641)_7 &= 1 + 4\cdot7 + 6\cdot7^2 + 4\cdot7^3 + 7^4\\ &= (1 + 7)^4,\end{aligned}$$

so its positive square root is $(1 + 7)^2 = 1 + 2\cdot7 + 1\cdot7^2$, which in base 7 is 121.

Also solved by John Hampton (The Open University), J. Kleeman (The College, Winchester), M. W. Friend (Gonville and Caius College, Cambridge).

9.5. The triangle T_1 lies inside the triangle T_2. Show that the perimeter of T_1 is shorter than that of T_2.

Solution

Denote the vertices of T_1 by A, B, C and those of T_2 by X, Y, Z. First produce AB to cut sides of T_2 in A', B'. (If A, B both lie, say, on the side XY, then take A', B' to be X, Y.) By the triangle inequality,

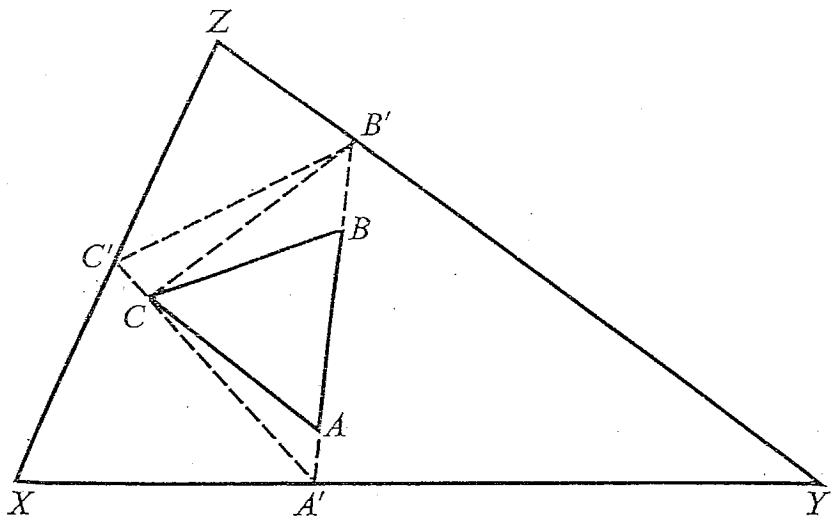


Figure A

$$\begin{aligned}\text{per } ABC &= AB + BC + CA\\ &\leqslant AB + BB' + B'C + CA' + A'A\\ &= \text{per } A'B'C.\end{aligned}$$

Next we produce $A'C$ to meet a side of T_2 in C' (as well as A'). Then

$$\begin{aligned}\text{per } A'B'C &= A'B' + B'C + CA'\\ &\leqslant A'B' + B'C' + C'C + CA'\\ &= \text{per } A'B'C'.\end{aligned}$$

We now have one of the following two situations (except that relabelling may be necessary). In the former case,

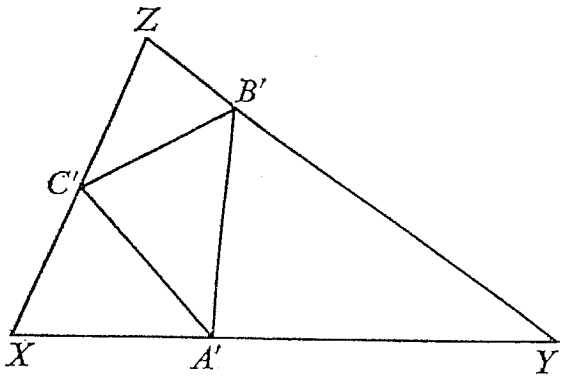


Figure B1

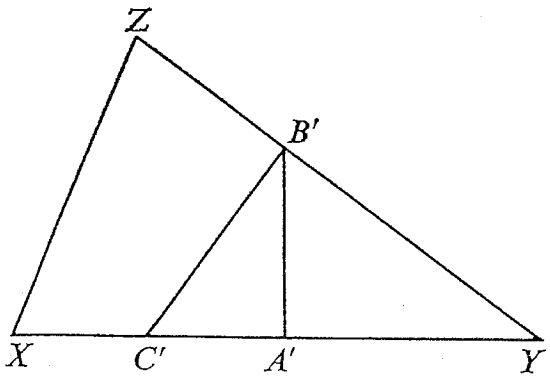


Figure B2

$$\begin{aligned}\text{per } A'B'C' &= A'B' + B'C' + C'A' \\ &\leqslant A'Y + YB' + B'Z + ZC' + C'X + XA' \\ &= \text{per } XYZ,\end{aligned}$$

and a similar inequality can be established in the latter case. Hence

$$\text{per } ABC \leqslant \text{per } XYZ.$$

Moreover, this inequality will be strict except when T_1 and T_2 are the same.

Also solved by M. W. Friend.

9.6. (i) Let (b_n) be a sequence of complex numbers such that $b_{n+1} - b_n \to l$ as $n \to \infty$. Show that $b_n/n \to l$ and that $|b_{n+1}| - |b_n| \to |l|$ as $n \to \infty$.

(ii) Let (a_n) be a sequence of non-zero real numbers, and put $b_n = a_{n+1}/a_n$ for $n = 1, 2, 3, \ldots$. Put $c_n = b_{n+1} - b_n$, $c'_n = |b_{n+1}| - |b_n|$. Show that it is possible for c'_n to tend to zero as $n \to \infty$ but for the sequence (c_n) to diverge.

Solution

(i) Let $\varepsilon > 0$. Then there exists N such that

$$|b_{n+1} - b_n - l| < \varepsilon/2 \text{ wherever } n \geqslant N.$$

Let $n > N$. Then

$$\begin{aligned}|b_n - b_N - (n-N)l| &= |(b_n - b_{n-1} - l) + (b_{n-1} - b_{n-2} - l) + \cdots + (b_{N+1} - b_N - l)| \\ &\leqslant |b_n - b_{n-1} - l| + |b_{n-1} - b_{n-2} - l| + \cdots + |b_{N+1} - b_N - l| \\ &< (n-N)(\varepsilon/2) \\ &< n\varepsilon/2.\end{aligned}$$

Then

$$\left|\left(\frac{b_n}{n} - l\right) + \frac{Nl - b_N}{n}\right| < \frac{\varepsilon}{2},$$

so

$$\left|\frac{b_n}{n} - l\right| - \left|\frac{b_N - Nl}{n}\right| < \frac{\varepsilon}{2},$$

$$\left|\frac{b_n}{n} - l\right| < \frac{\varepsilon}{2} + \left|\frac{b_N - Nl}{n}\right|.$$

If we now take $n \geqslant \max\{N, 2|b_N - Nl|/\varepsilon\}$, we obtain

$$\left|\frac{b_n}{n} - l\right| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

This shows that $b_n/n \to l$ as $n \to \infty$.

Now put

$$(b_n/n) - l = \varepsilon_n, \quad b_{n+1} - b_n - l = \eta_n.$$

Then $\varepsilon_n, \eta_n \to 0$ as $n \to \infty$, and

$$b_{n+1} - b_n + \varepsilon_n - \frac{b_n}{n} = \eta_n,$$

$$b_{n+1} = \frac{n+1}{n} b_n + \eta_n - \varepsilon_n,$$

from which

$$|b_{n+1}| \leqslant \frac{n+1}{n} |b_n| + |\eta_n| + |\varepsilon_n|.$$

Thus

$$|b_{n+1}| - \frac{n+1}{n} |b_n| \to 0 \quad \text{as } n \to \infty.$$

But $b_n/n \to l$ as $n \to \infty$, so $|b_n|/n \to |l|$ as $n \to \infty$. Hence

$$|b_{n+1}| - |b_n| = \left(|b_{n+1}| - \frac{n+1}{n} |b_n| \right) + |b_n|/n \to |l| \quad \text{as } n \to \infty.$$

(ii) Take $(a_n) = (1, 1, -1, -1, 1, 1, \ldots)$. Then $b_n = (-1)^{n+1}$, $c_n = 2(-1)^n$, $c'_n = 0$.

Book Reviews

Calculus Applicable. School Council Sixth Form Mathematics Project. Heinemann Educational Books Ltd, London, 1976. Pp. viii + 124. £1·90 paperback.

This is one of a series of books designed to meet the needs of today's sixth-former.

The book is intended for individualised learning and is set at 0 or A/0 level. Students are expected to be familiar with the idea of a polynomial, limit and gradient, also with the binomial expansion and the summation notation. The approach is via modelling and there are numerous references to the 52-page section of background material, mathematical notes, hints and answers.

There are sections on speed, gradient, applications of differentiation, rates of change, greatest and least values, integration, areas and volumes; finally there is a consolidation chapter.

The book differs from other books at this level in two respects: the approach, which takes a problem, discovers the necessary mathematics, solves the problem and proceeds to further applications; and the problems themselves, which are designed to show the relevance and applicability of the calculus and cover such diverse areas as coffee percolators and lunar modules.

The book is well printed and easy to read. There is little in it for the serious student of mathematics, but it should be well suited to its intended audience. Staff may wish to have a copy, for its new approach and different type of questions make a refreshing change from the more standard texts.

Benfield School, Newcastle upon Tyne T. R. FERGUSON

Functions of a Complex Variable. By D. O. TALL. Routledge & Kegan Paul, London, 1977 (first published 1970). Pp. 80. £1·75.

In the theory of complex-valued functions of a complex variable, the ideas of continuity and differentiability generalise easily from the real case, but the latter especially is deceptive. Complex differentiability is a very strong assumption, and correspondingly strong theorems are obtained. For example, if a complex function is assumed differentiable just once everywhere in its domain of definition, then all higher derivatives automatically exist. In addition, such a function is completely determined by its values along any curve in the complex plane. It follows from this, for example, that z^2 is the only complex differentiable function which agrees with x^2 on the real axis.

These results (and others) are obtained in the first half of *Functions of a Complex Variable* by using the theory of complex integration along contours. The complex analogue of the Fundamental Theorem of Calculus is used to give a natural approach to Cauchy's Theorem which leads to Taylor's Theorem and the results mentioned in the first paragraph.

The second half of the book contains applications of the theory, including conformal mappings, harmonic functions, calculation of integrals by residues, together with a description of analytic continuation and Riemann surfaces.

The whole subject offers a nice blend of theory and calculation, and this is well presented in this book. The exposition is sufficiently rigorous for a special honours mathematics student, but it is also suitable for scientists and engineers who may be principally concerned with results and techniques. Formally the only prerequisite is a knowledge of complex numbers; however for a real understanding of the book what is needed is an appreciation of the basic analysis that is usually taught in first-year university mathematics courses.

University of Durham J. BOLTON

Statistical Theory (3rd Edition). By B. W. LINDGREN. Collier–Macmillan, London, 1976. Pp. xiii+614. £6·00.

This well-known book on the mathematical theory of statistics is designed for a one-year undergraduate course of three lectures per week for specialist students. This purpose it fulfils thoroughly and competently. The third edition differs from the second in several important respects. The section on decision theory has been moved from its position as a preface for statistical problems; it has been expanded and comes in later as a chapter in its own right. This change brings the presentation of estimation and hypothesis testing more in line with the historical development of these ideas. The section on the bivariate normal distribution, previously with the univariate normal, is now in a new chapter on multivariate distributions. There is also a new chapter on the analysis of categorical data to precede work on non-parametric inference.

At today's prices this book is good value for money and can be recommended not only to its intended readership, but also to sixth-form teachers interested in the theoretical background of their subject.

University of Sheffield P. HOLMES

Notes on Contributors

J. G. Brennan is a Lecturer in Pure Mathematics at the University College of Swansea. Although originally an algebraic geometer, his interests in recent years have centred in combinatorics.

Michael Atkinson read mathematics at Queen's College, Oxford. There he subsequently also wrote his doctoral thesis, which was on group theory. Since 1970 he has been a Lecturer in the Department of Computing Mathematics at University College, Cardiff. His research interests are in the theory of algorithms and in algebra, especially in computer applications to group theory.

S. Bookchin had no formal mathematical education but, throughout his life, he has had a deep love of numbers. Some time after the First World War he settled in Palestine (now Israel) and worked as a building labourer. Studying on his own, he has rediscovered many results belonging to the theory of numbers.

M. Lewin is an Associate Professor of Mathematics at the Technion in Haifa. His main interests are in combinatorics and graph theory. During the years 1967 to 1969, he was a Visiting Lecturer in the Mathematics Department of the University of Reading.

John Strange was an undergraduate at Queens' College, Cambridge. After taking the Mathematical Tripos he went to a school near Paris as English Assistant. He subsequently took a post teaching English and mathematics at a school in central France, and then taught mathematics for eight years in Malta. He is now teaching French and mathematics at Goring Hall School.

Contents

ISSN 0025–5653

PRICES (*postage included*)

Prices for Volume 10 (*Issues Nos.* 1, 2, *and* 3):

Subscribers in Britain and Europe: £1·15
Subscribers overseas: £2·30 (US$4.00; $A3.70)
(These prices apply even if the order is placed by an agent in Britain.)
A discount of 10% is allowed on all orders for five or more copies.

Back issues:

Volume 1 is out of print. All other back issues are still available; information concerning prices may be obtained from the Editor.

Enquiries about rates, subscriptions and advertisements should be directed to:

Editor—*Mathematical Spectrum*,
Hicks Building,
The University,
Sheffield S3 7RH, England.

Printed in England by Galliard (Printers) Ltd, Great Yarmouth