Eureka Editor
archim-eureka@srcf.net
The Archimedeans
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WA
United Kingdom

Published by The Archimedeans, the mathematics student society of the University of Cambridge

Thanks to the Betty & Gordon Moore Library, Cambridge

EUREKA

THE ARCHIMEDEANS' JOURNAL

NUMBER 35

OCTOBER 1972 PRICE 20p

Editor: **JOSEPH CONLON**

Business Manager: **BRYAN LOSE**

Contents

EUREKA

The Journal of the Archimedeans (Cambridge University Mathematical Society)

NUMBER 35 OCTOBER 1972

Correspondence for *Eureka* should be addressed to: The Editor (or Business Manager), "Eureka", The Arts School, Bene't Street, Cambridge, England.

Postal rates: 24p unless £1.00 or more sent in advance in which case accounts will be debited at 20p per issue (corresponding dollar rates are 80c per copy or 70c if more than $4.00 sent in advance. The attention of overseas subscribers is drawn to the fact that it costs *Eureka* 60c for every cheque cashed drawn on a foreign bank).

Back numbers on request: few before 1960—xeroxed copies at 65p if not available.

The editor would like to thank all those who have helped in the production of this issue, especially my predecessor Ian McCredie, Bryan Lowe, Dr. G. K. Eagleson, Malcolm Pemberton and Bernard Walters.

Editorial

Number 1073 took a last look at the familiar outline of the city which, until a few hours ago, had been his home. It was called Camathica now — its original name, like his own, he had forgotten years ago. In fact, at this final hour of victory over The System he felt like going back and giving himself up to the dreaded Tripox police. His thoughts wandered to the future. Perhaps he might not be able to cope without the endless rantings of Agit Ramanjau Mistrat and the rest of the inner clique about the virtues of R and F (as the new super-efficient vocabulary had it).

The notion quickly fled his mind. There was no bitterness in his heart towards The System. After all it was just a monolithic machine, self-perpetuating with no ultimate goal in mind except "perfection, perfection, perfection" as he used to hear so often.

Now, in the silence of the summer evening, 1073 tried to think what it was like before The System. He remembered the autumn of 1970 well when he had first arrived in Camathica.

The people were docile and the elders of the city showed their appreciation of this. An atmosphere of benevolent despotism reigned and so the tide of revolt which had spread across neighbouring cities left Camathica untouched. Like all the arrivals he got his copy of *Varsity* and there on page 164 was what he was looking for. The small advertisement ran, "Socialist Mathematicians League–The group is in the process of formation . . . ". Here was an opportunity to build up a moderate reforming movement, which would seek to fuse new ideas to ancient traditions. Unfortunately the movement died at its inception. The leaders claimed they had not been serious. All they wanted was a car. Little did they realise that they had missed the last chance to pull back from the brink of the cataclysm which was to follow.

After that there was a blank in the memory of 1073; and then, the all-pervading voice of The System.

An Alphametric

Solve the following pair of additions.

THIS	THIS
IS	IS
A	1996
LEAP	
YEAR	

(Every letter represents a different digit, and there are 2 solutions)

(Solution on page 54.)

Prime Numbers and Brownian Motion

The 1972 Rouse Ball Lecture

by Professor P. BILLINGSLEY, *University of Chicago*

Because it factors into a product of prime numbers, each integer contains within it a kind of Brownian motion path, and the mathematics of Brownian motion can be used to derive results about the factorization. I am aware of the ancient and lamentably persistent notion that a theorem stated in probability language is rather less true than it might otherwise be. I shall nevertheless state these theorems in probability language and even give them probabilistic proofs, thereby rendering them wholly false in the eyes of those who hold to the ancient view I speak of.

There will be little in the way of proofs anyway, since for the most part I shall only illustrate general theorems by examples and special cases. For this I have the authority of William Feller. When I was his student at Princeton, he used to say that the best in mathematics, as in art, letters, and all else—that the best consists of the general embodied in the concrete. Although for some time I took that to be an anti-military sentiment, I did eventually understand it as the intellectual-esthetic principle he intended, and I have tried ever since to keep it somewhere near the front of my mind.

Brownian Motion

Imagine suspended in a fluid a particle bombarded by molecules moving about in their wonted fashion. The particle will perform that irregular and seemingly random motion first described by Robert Brown in 1828. Since we shall be concerned with just one component of this motion, imagine it projected on a vertical axis: At each instant t of time we note the height $x(t)$ of the particle above a fixed horizontal plane. Over one unit of time, the motion of the particle, which we take to start at 0, is described by the positions $x(t)$ for $0 \leqslant t \leqslant 1$—that is, by a continuous function x on $[0,1]$ with $x(0) = 0$. This leads us to consider the collection $C = C_0[0,1]$ of such functions x.

For technical reasons, we make C into a metric space by taking the distance between two of its elements to be the maximum vertical distance between their graphs. This topology, called the uniform

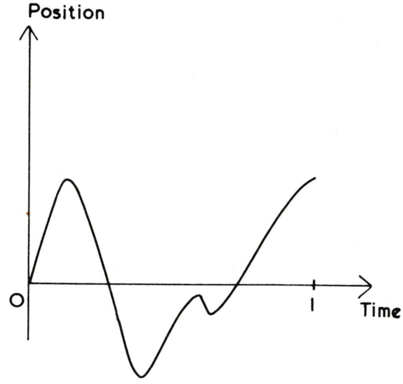


Figure 1

topology, is of little direct concern here; it is brought in mostly as evidence that the discussion to follow does have a mathematical basis.

The random motion of the particle is described by an assignment of

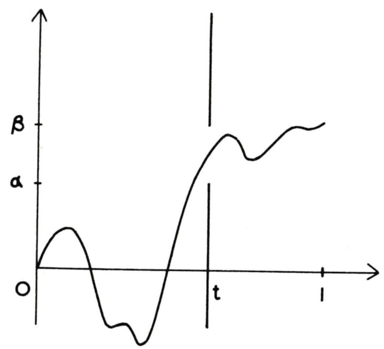


Figure 2

probabilities $P(A)$ to subsets A of C; $P(A)$ represents the chance that the path traced out by the particle lies in A, or is represented by a function x that lies in A. The set $[x\colon \alpha \leqslant x(t) \leqslant \beta]$, consisting of the paths that go through the gate in Figure 2, represents the event that at time t the particle will lie between α and β; it is assigned probability

$$(1) \qquad P[x: \alpha \leqslant x(t) \leqslant \beta] = \frac{1}{\sqrt{2\pi t}} \int_{\alpha}^{\beta} e^{-u^2/2t}\, du.$$

Thus the distribution of the position at time t follows the Gaussian curve with mean 0 and variance t. That the mean is 0 reflects the fact that the particle is as likely to go up as to go down: There is no drift. The variance t grows linearly: This reflects the fact that the particle tends to wander away from its starting point and having done so suffers no force tending to restore it to that starting point. The equation (1) can be extended so as to describe the distribution of the increment over any interval of time.

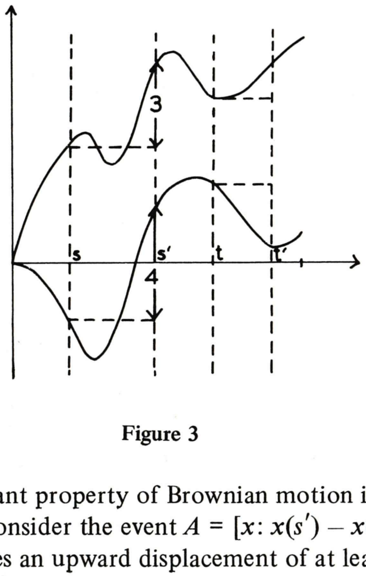


Figure 3

The other important property of Brownian motion is this: Suppose $s < s' < t < t'$, and consider the event $A = [x: x(s') - x(s) \geqslant 3]$ that the particle undergoes an upward displacement of at least 3 units during the time interval $[s,s']$, together with the event $B = [x: x(t') - x(t) < 0]$ that the particle undergoes a downward displacement during the time interval $[t,t']$. For example, the top path in Figure 3 lies in A but not in B, and the bottom path lies both in A and in B. The probabilities of A and B and of their intersection $A \cap B$ are related by

$$(2) \qquad P(A \cap B) = P(A)P(B).$$

Thus A and B satisfy the definition of independence, which reflects the fact that the displacement the particle undergoes during $[s,s']$ in no way influences the displacement it undergoes during $[t,t']$. This implies a kind of lack of memory: Although the future behavior of the particle depends on its present position, it does not depend on how the particle got there. Equation (2) has a more general form showing that the increments over any number of disjoint intervals are independent.

The equations (1) and (2), together with generalized versions of them, determine all the probabilities $P(A)$. (This ignores a technical point: $P(A)$ cannot be defined for every subset A of C, but it can for every Borel set A—that is, for every A in the σ-field generated by the sets open in the uniform topology.) It was one of Norbert Wiener's achievements to prove that there does exist an assignment of probabilities satisfying these rules, and P (the corresponding measure on the Borel sets) is accordingly called Wiener measure.

Wiener measure, set up to reflect by (1) and (2) the characteristics of Brownian motion, has some startling properties. If A is the set of paths of unbounded variation, then $P(A) = 1$. At this point physicists lose interest, because of their obsessive concern with reality, together with the fact that a path of unbounded variation represents the motion of a particle that in its wanderings back and forth travels an infinite distance. But the fact is mathematically interesting, and so is the fact that $P(A) = 1$ if A is the set of x in C that are nowhere differentiable. Constructing a continuous, nowhere differentiable function is difficult, but drawing an element from C randomly according to P produces such a function with probability 1.

In what follows, we shall be concerned with sets that correspond more closely with reality. Suppose $\alpha \geqslant 0$ and consider the event $[x\colon \max x(t) \geqslant \alpha]$ that the particle achieves the height α at some time t with $0 \leqslant t \leqslant 1$. First, $P[x\colon \max x(t) \geqslant \alpha] = P[x\colon \max x(t) \geqslant \alpha \;\&\; x(1) \geqslant \alpha] + P[x\colon \max x(t) \geqslant \alpha \;\&\; x(1) \leqslant \alpha]$. The two probabilities on the right here can be proved equal, roughly because once the particle achieves the height α it is as likely to wander upward and finish above α at time 1 as to wander downward and finish below α. Thus $P[x\colon \max x(t) \geqslant \alpha] = 2P[x\colon \max x(t) \geqslant \alpha \;\&\; x(1) \geqslant \alpha]$. Since the condition $\max x(t) \geqslant \alpha$ is superfluous in the presence of the condition $x(1) \geqslant \alpha$, the right side here is $2P[x\colon x(1) \geqslant \alpha]$, and (1) with $t = 1$, $\alpha \geqslant 0$, and $\beta = \infty$ now implies

$$(3) \qquad P[x\colon \max x(t) \geqslant \alpha] = \frac{2}{\sqrt{2\pi}} \int_{\alpha}^{\infty} e^{-u^2/2}\, du.$$

Although making it rigorous requires some effort, this derivation of (3) is intuitive. The next result will be stated without any proof. Like many *ex cathedra* assertions, it runs counter to intuition. Consider the set $[t: x(t) > 0]$ of time points $t, 0 \leqslant t \leqslant 1$, for which the particle is above 0. This set is a union of intervals (infinitely many, contrary to Figure 4). Denote by bars the Lebesgue measure of this set, the sum of

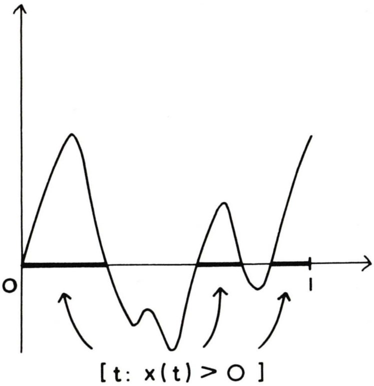


Figure 4

the lengths of the constituent intervals: $|[t: x(t) > 0]|$. The distribution of this quantity, the total time spent above 0, is given by

$$P[x: \alpha \leqslant |[t: x(t) > 0]| \leqslant \beta] = \frac{1}{\pi} \int_{\alpha}^{\beta} \frac{du}{\sqrt{u(1-u)}} \tag{4}$$

for $0 \leqslant \alpha \leqslant \beta \leqslant 1$. This is Paul Lévy's arc sine law, so called because carrying out the integration involves the arc sine function.

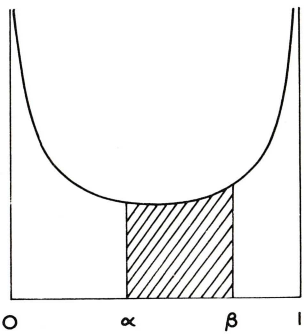


Figure 5

Figure 5 shows the shape of the density, the area of the shaded region representing the right side of (4). The curve is U-shaped, so that if the length $\beta - \alpha$ of the interval is fixed, the probability grows as the interval nears 0 or 1, being smallest when the interval is centered on 1/2. This is strange because the time spent above 0 has mean 1/2 by symmetry, and ordinarily values near the mean of a random quantity are more likely to occur than are values far removed from the mean, whereas here the situation is just the opposite.

Random Walk

Imagine a particle moving about at random on the nodes of a cubic lattice. The particle can move in any of six directions (North, South, East, West, Up, Down) to an adjacent node. The direction is determined by the roll of a balanced die, the particle moves to the next node, and the die is rolled once more to determine the direction of the next move, and so on. Figure 6 shows five steps of such a random walk, together

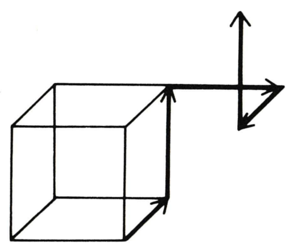


Figure 6

with one of the cells of the cubic lattice. The figure is in the spirit of a venerable vector analysis book which began a proof of Gauss's theorem by enjoining the reader to consider "an infinitesimal element of volume of dimensions dx, dy, and dz". This injunction was accompanied by a nicely labelled diagram like Figure 7, which was said to show such an infinitesimal element of volume "much enlarged". Well, Figure 6 is much enlarged too, and if the cubes of the lattice are really very small and the particle moves very rapidly from node to node it is natural to expect the motion to approximate Brownian motion.

We shall explore a one-dimensional version of this idea. Consider a vertical axis with the integer points $0, \pm 1, \pm 2, \ldots$ marked off on it. We start at 0, toss a coin, and move upward one unit if the coin falls heads and downward one unit if the coin falls tails. In the new position ($+1$ or -1), we toss the coin again and move up or down one unit according as it falls heads or tails, and we continue this way for k

steps. If we take one unit of time to execute each step of the random walk and proceed at a uniform rate from one node to the next, our progress is described by a function like that in Figure 8, a polygonal path whose height over i is the position at i—that is, the position after the ith step.

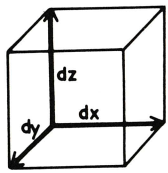


Figure 7

This path can also be viewed as describing the fluctuations in a gambler's fortune. The position on the vertical axis represents the gambler's fortune (relative to his initial capital, so that he starts conventionally at 0), and it moves up or down one unit—say one pound—according as he wins or loses the next play.

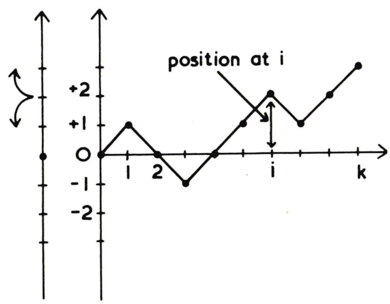


Figure 8

The random-walk path has some of the properties of Brownian motion. In the first place, if $i < i' < j < j'$, the displacements undergone over the time intervals $[i,i']$ and $[j,j']$ are independent because they depend on different sets of tosses and the tosses are assumed independent (the coin has no memory). Thus the path has essentially independent increments (for intervals with nonintegral endpoints the increments may not be exactly independent). The distance moved in one step has mean

(5) $\quad \frac{1}{2}(+1) + \frac{1}{2}(-1) = 0$

and variance

(6) $\quad \frac{1}{2}(+1)^2 + \frac{1}{2}(-1)^2 = 1,$

and so the position at i has mean 0 and by independence has variance i, another property of Brownian motion (see equation (1)). Although the polygonal character of the path is not shared by Brownian motion, a suitable contraction of the time scales will make the straight-line segments in Figure 8 disappear in the limit as $k \to \infty$.

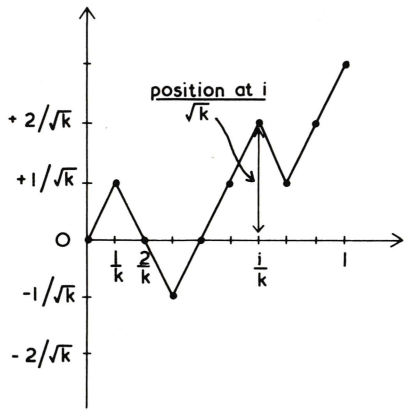


Figure 9

Suppose we contract the time scale by a factor k and contract the vertical scale by a factor $\sqrt{k}$, passing from Figure 8 to Figure 9. This preserves the essential independence of the increments. The height of the new path over the point i/k, being $1/\sqrt{k}$ times the height of the old position after step i, has mean 0; its variance is $(1/\sqrt{k})^2$ times the old variance i and hence has value i/k. Contracting time by the factor k gives us a path defined over $[0,1]$, in other words an element of C. The vertical rescaling by $1/\sqrt{k}$ makes the variances work out right.

The random path in Figure 9 has the essential properties of Brownian motion. Since as $k \to \infty$ the links in the polygon will vanish, we can hope to have a Brownian motion in the limit. And indeed

(7) $\quad \text{Prob}\,[\text{path} \in A] \to P(A) \qquad (k \to \infty)$

for subsets A of the space C, where $P(A)$ is Wiener measure. There are 2^k paths like the one in Figure 9, and Prob [path $\in A$] is 2^{-k} times the number of them that lie in A.

Suppose the A in (7) is the set $[x\colon \alpha \leqslant x(1) \leqslant \beta]$ of paths in C that over the point $t = 1$ have a height between α and β. Since the height over $t = 1$ in Figure 9 is $1/\sqrt{k}$ times the position at k in the original random walk, (7) and (1) together imply

$$\text{(8)} \qquad \text{Prob}\left[\alpha \leqslant \frac{\text{position at } k}{\sqrt{k}} \leqslant \beta\right] \to \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\beta} e^{-u^2/2}\, du.$$

This, the De Moivre-Laplace central limit theorem for Bernoulli trials, describes the position after a large number of steps in a random walk, or the gambler's fortune at the end of an evening's play of k steps. If $\alpha = \beta = \cdot 9$, the integral in (8) is about $\cdot 6$. If $k = 100$, the gambler thus has probability approximately $\cdot 6$ of ending the evening within $9 \times \sqrt{100} = 9$ pounds of his initial capital.

Suppose now that A is the set in (3), the set of paths in C having somewhere a height of α or greater (here $\alpha \geqslant 0$). The path in Figure 9 lies in A if at some time during the evening's play the gambler's fortune is at least $\alpha\sqrt{k}$ pounds above his initial capital, and by (7) this converges to the integral in (3). The integral is about $\cdot 1$ for $\alpha = 1{\cdot}7$. With $k = 100$, this gives an approximate probability of $\cdot 1$ that the gambler will have been at least 17 pounds ahead at the time he should have quit.

Finally, suppose A is the set $[x\colon \alpha \leqslant |[t\colon x(t) > 0]| \leqslant \beta]$ in (4). During the evening, the gambler is ahead a certain fraction of the time; if the curve in Figure 9 represents the history of his fortunes, it is in the set A if this fraction lies between α and β. The chance of this event is by (7) and (4) about equal to the area of the shaded region in Figure 5. The chance the gambler is ahead more than 90% of the time turns out to be about $\cdot 2$, whereas the chance that he is ahead between 45% and 55% of the time is only about $\cdot 06$. In one evening in five the gambler will be ahead more than 90% of that evening's play. By symmetry, in one evening in five the gambler will be ahead less than 10% of that evening's play. To convince him in the first [second] case that his experience is due merely to chance and not to his being Fortune's favorite [Fortune's fool] will be difficult [impossible].

We have applied (7) to three interesting sets A. If A is the set of continuous functions of unbounded variation, then $P(A) = 1$, as explained above, while Prob [path $\in A$] $= 0$ because the curve in Figure 9 is visibly of bounded variation. Thus (7) fails for certain subsets A of C. The mathematical fact is that (7) holds for every set (Borel set) A whose boundary ∂A (boundary in the sense of the uniform topology) satisfies $P(\partial A) = 0$, a condition which holds in our three applications. The proof of the theorem uses a combination of probability theory and functional analysis. (Details can be found in my book *Convergence of Probability Measures*.)

Having used Brownian motion in some problems of random walk and gambling, we shall now use Brownian motion, random walk, and gambling in some problems of multiplicative arithmetic.

Prime Divisors

For a positive integer n, let $f(n)$ be the number of distinct prime factors it contains. We do not count multiplicity: $f(3^4.5^2)$ is 2, not 6. The table shows some values of the function f. It rises slowly. The

n	2	3	4	5	6	7	$\cdots$	29	30	31	$\cdots$	209	210	211	$\cdots$
$f(n)$	1	1	1	1	2	1	$\cdots$	1	3	1	$\cdots$	2	4	1	$\cdots$

smallest n's with respective f-values 2, 3, and 4 are $2.3 = 6$, $2.3.5 = 30$, and $2.3.5.7 = 210$. The fact that there are infinitely many primes implies that f assumes arbitrarily large values; it also implies that f infinitely often drops back to 1, since $f(p) = 1$ for prime p.

Since f varies in this irregular fashion, it is natural to ask after its average behavior. For example, it can be shown that

$$(9) \qquad \frac{1}{N} \sum_{n=1}^{N} f(n) \sim \log \log N.$$

Since $\log \log 10^{70} \approx 5$, the typical integer under 10^{70} has a mere five prime divisors. More delicate questions concern the distribution of f. If S is a set of positive integers, let $P_N(S)$ be the fraction among the integers $1, 2, \ldots, N$ that lie in S:

$$(10) \qquad P_N(S) = \frac{1}{N} \times \#\,[n\colon 1 \leqslant n \leqslant N \;\&\; n \in S].$$

The problem now is to get information about quantities like $P_N[n\colon a \leqslant f(n) \leqslant b]$.

Now (10) can be viewed as a probability: We draw an integer n at random from the range $1 \leqslant n \leqslant N$, and $P_N(S)$ is the probability that it will lie in S. That $P_N[n\colon a \leqslant f(n) \leqslant b]$ can be viewed as a probability does not, if you will believe me, by itself ensure that probability theory will help in the evaluation. In fact it does help because the notion of independence can be brought to bear. If $\delta_p(n)$ is 1 or 0 according as the prime p divides n or not, then $f(n) = \Sigma_p \delta_p(n)$. We can understand the distribution of $f(n)$ if we understand the joint behavior of the $\delta_p(n)$ as random quantities.

The number of multiples of p up to N is the integral part $[N/p]$ of N/p. The probability that $\delta_p(n) = 1$, or that $p | n$, is thus

$$P_N[n: p|n] = \frac{1}{N}\left[\frac{N}{p}\right] \approx \frac{1}{p}, \tag{11}$$

the approximation valid for large N. This reflects the fact that p divides every pth integer, and it does not require that p be prime.

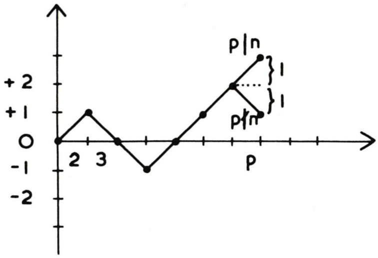


Figure 10

Distinct primes p and q individually divide n if and only if their product pq divides n, so that

$$\begin{aligned} P_N[n: p|n \ \&\ q|n] &= P_N[n: pq|n] \approx \frac{1}{pq} \\ &= \frac{1}{p}\cdot\frac{1}{q} \approx P_N[n: p|n]\cdot P_N[n: q|n]. \end{aligned} \tag{12}$$

Thus the events $[n: p|n]$ and $[n: q|n]$ approximately satisfy the definition of independence if n is random, $1 \leqslant n \leqslant N$, with N large.

We can use this fact to construct a kind of random walk path containing information about the prime factorization of n and in particular about $f(n)$. On a vertical axis with the integer points marked off, we start at 0 and go up a unit if $2|n$ and down a unit if $2\nmid n$. From our new position (+1 or -1), we go up a unit if $3|n$ and down a unit if $3\nmid n$. We proceed in this way, examining each prime in succession. Figure 10 describes this factorization random walk in the same way that Figure 8 describes the coin-tossing random walk. Each number on the time axis is the prime corresponding to that step in the random walk. We consider later how long to continue the walk.

Since n is random, this path is random. But since all the randomness is in the drawing of n before the walk starts, the factorization random walk may seem less random than the coin-tossing random walk. This is an illusion. We may imagine tossing the coin k times in advance of the walk, recording the sequence of heads and tails, and only then performing the corresponding walk. The walk would be a bore, since we would see its whole history on record before setting out. So imagine a friend who tosses the coin k times, records the results in advance of the journey, and reveals the outcomes to us one by one as we execute the walk. This restores the suspense. For the factorization random walk, we can imagine a friend who draws n at random, $1 \leqslant n \leqslant N$, factors n into primes, and at each step of the walk tells us whether or not the corresponding p divides n.

The increment of the random path in Figure 10 over an interval depends on how many in the corresponding set of primes divide n. Increments over disjoint intervals depend on disjoint sets of primes and hence by (12) the increments will be approximately independent if N is large. Unlike Brownian motion, however, the factorization random walk has a strong downward drift. By (11), the chance of going downward is about $1 - 1/p$, which is almost 1 for large p. The remedy is to move up a distance $1 - 1/p$ if $p \mid n$ and to move down a distance $1/p$ if $p \nmid n$. The expected distance moved is now approximately

$$\frac{1}{p}\left(1 - \frac{1}{p}\right) + \left(1 - \frac{1}{p}\right)\left(-\frac{1}{p}\right) = 0.$$

This compares with (5), an equation which shows that the coin-tossing random walk has no drift.

The variance of the distance moved is now approximately

$$\frac{1}{p}\left(1 - \frac{1}{p}\right)^2 + \left(1 - \frac{1}{p}\right)\left(-\frac{1}{p}\right)^2 = \frac{1}{p}\left(1 - \frac{1}{p}\right) \approx \frac{1}{p}.$$

The distance moved in the step corresponding to p thus tends to be small for large p, in contrast with the coin-tossing random walk, which by (6) proceeds with vigour ever undiminished. The remedy this time is to spend only an amount $1/p$ of time executing the step corresponding to p. With these two modifications, the path is as in Figure 11. To recapitulate, over an interval of length $1/p$, the path rises linearly an amount $\delta_p(n) - 1/p$—that is, rises $1 - 1/p$ if $p \mid n$ (approximate probability $1/p$) and rises $0 - 1/p$ if $p \nmid n$ (approximate probability $1 - 1/p$).

The point T in the figure (the right endpoint of the interval corresponding to p) is $\Sigma_{q \leqslant p}\ 1/q$ (sum over primes q not exceeding p), which can be shown to be very close to $\log \log p$ (see (9)). The height

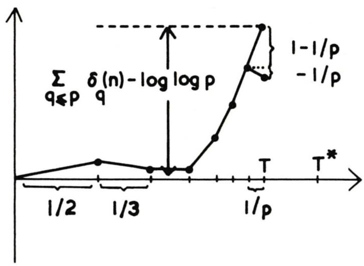


Figure 11

of the curve over T is $\Sigma_{q \leqslant p}\ (\delta_q(n) - 1/q) \approx \Sigma_{q \leqslant p}\ \delta_q(n) - \log \log p$. We continue the walk until each $p \leqslant N$ has been dealt with, and the corresponding point on the time axis is $T^* = \Sigma_{p \leqslant N}\ 1/p \approx \log \log N$.

The random path now resembles a coin-tossing path in that the increments are almost independent (for large N), there is essentially no drift, and the variances are about right. As in the coin-tossing case,

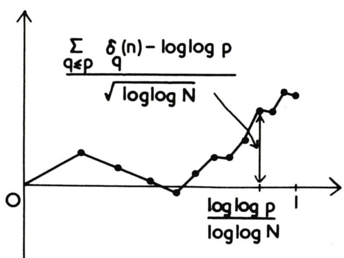


Figure 12

rescaling will lead in the limit ($N \to \infty$) to Brownian motion. To send T^* to the point $t = 1$, we contract the horizontal scale by a factor $\log \log N$, and, again as in the coin-tossing case, we contract the vertical scale by the square root of this. The point T in Figure 11 goes to $\log \log p / \log \log N$, and the path is that shown in Figure 12.

Since the path depends on n and N, denote it $\text{path}_N(n)$. Since n is random, so is the path, and the chance that it lies in a given subset A of the space C is $P_N[n: \text{path}_N(n) \in A]$. The theorem linking primes with Brownian motion is this: If A is a (Borel) subset of C satisfying $P(\partial A) = 0$, then

$$(13) \qquad P_N[n: \text{path}_N(n) \in A] \to P(A) \qquad (N \to \infty)$$

where P is Wiener measure. The proof of (13) uses a combination of probability theory, functional analysis, and number theory. (The theorem is given implicitly in Kubilius's book *Probabilistic Methods in the Theory of Numbers*, p. 122, explicitly in one of the manuscript versions of my "Convergence of Probability Measures", and in more general form in Philipp's forthcoming paper, "An invariance principle for additive number-theoretic functions".)

Consider the three sets A to which we applied the analogous result (7). Whether or not the path in Figure 12 lies in the set $A = [x: \alpha \leqslant x(1) \leqslant \beta]$ depends on its height over $t = 1$; this height is the quantity indicated in the diagram with N in place of p. Since $\Sigma_{q \leqslant N} \delta_q(n)$ is the total number $f(n)$ of distinct prime divisors of n, (13) together with (1) gives

$$(14) \qquad P_N\left[n: \alpha \leqslant \frac{f(n) - \log\log N}{\sqrt{\log\log N}} \leqslant \beta\right] \to \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta e^{-u^2/2}\, du.$$

This is the Erdös-Kac central limit theorem for f. (For an elementary treatment of (14), see *American Mathematical Monthly*, **76** (1969), 132.)

For $-\alpha = \beta = \cdot 9$, the integral in (14) is about $\cdot 6$, and if $N = 10^{70}$, so that $\log\log N \approx 5$, the double inequality in (14) is approximately the same as $\cdot 9 \leqslant (f(n) - 5)/\sqrt{5} \leqslant \cdot 9$, which in turn is approximately the same as $3 \leqslant f(n) \leqslant 7$. Thus about 60% of the integers under 10^{70} have from 3 to 7 prime divisors.

Applying (13) to the set in (3) gives the approximate distribution of the maximum of the curve in Figure 12. For each $p (p \leqslant N)$ we look at the number $\Sigma_{q \leqslant p} \delta_q(n)$ of prime divisors of n that do not exceed p, compare this with its value $\log\log p$ for a "typical" n, and compute the discrepancy (the difference). The integral in (3) being about $\cdot 1$ if $\alpha = 1 \cdot 7$, for about 10% of the integers under 10^{70} does the maximum of this discrepancy exceed $1 \cdot 7 \times \sqrt{5} \approx 3 \cdot 8$.

And consider once again the set in (4). Whether or not the curve in Figure 12 lies in this set depends on the amount of time it is above 0. The polygonal segment corresponding to p has length $p^{-1}/\log\log N$

when projected on the horizontal axis, and so the amount of time above 0 is essentially

$$(15) \qquad \Sigma\left[\frac{1}{p \log\log N} : p \leqslant N \;\&\; \sum_{q \leqslant p} \delta_q(n) > \log\log p\right],$$

the sum extending over those $p(p \leqslant N)$ for which n contains excessively many prime factors to the left of p. For large N, the distribution of (15) approximately follows the density curve in Figure 5. For about 20% of the integers under N it exceeds ·9, and for about 6% it lies between ·45 and ·55.

Prime factors exhibit in this respect the strange behavior coins do. In a way they are even more strange. A quantity perhaps more natural to consider than (15) is

$$(16) \qquad \frac{1}{\pi(N)} \times \#\left[p : p \leqslant N \;\&\; \sum_{q \leqslant p} \delta_q(n) > \log\log p\right],$$

the *number* of p for which n contains excessively many primes to the left of p, normalized by division by $\pi(N)$, the total number of primes involved. For N large, of the break points in the polygon in Figure 12 the great majority are very near 1, with the result that in the limit the distribution of (16) consists of a mass of ·5 at 0 and a mass of ·5 at 1. If $\epsilon > 0$ and N exceeds some N_ϵ, then (16) is less than ϵ with a probability lying between $\cdot 5 - \epsilon$ and $\cdot 5 + \epsilon$ and is greater than $1 - \epsilon$ with a probability lying in the same range.

Two Problems

1 (A) If the probability of picking up a bridge hand containing 13 spades is p, what is the probability of picking up a bridge hand with 14 points and 4–4–4–1 distribution?
(B) A black knight and a white queen are placed randomly on different squares of a chess board. What is the probability that one can capture the other?

2 Define $S(n) = \dfrac{10^n - 1}{9}$
i.e. the number with n digits 1.
Prove that for infinitely many n, n divides $S(n)$.
Hint: $n < S(n)$ if $n > 1$.

(Solutions on page 54.)

Relativistic Doppler Effect for Photons

by Professor D. R. BATES, *Queen's University, Belfast*

"There are nine and sixty ways of constructing tribal lays,
And every single one of them is right!"

(From *In the Neolithic Age*
by Rudyard Kipling)

Just half a century ago Erwin Schrödinger (*Physik. Zeitschr.* 22, 301, 1922) showed that the relativistic Doppler effect is a consequence of the conservation of energy and momentum in the emission of a photon by an atom. Like the theory of the Compton effect, which was first presented in the same year, this was at the time of interest in providing a further example of the apparent paradox that radiation has the properties of particles as well as of waves.

Undoubtedly the Compton effect is best explained in terms of photons. The wave treatment is however the simpler in the case of the relativistic Doppler effect, and has the advantage that it depends directly on the Lorentz transformations. Most expositors either ignore the several photon aspects of the phenomenon or merely refer to one of them very briefly. Those who discuss a photon aspect fully rarely do so except after the special theory has been developed in some sophisticated form. On the fiftieth anniversary of Schrödinger's original paper it is worth recalling that only an elementary knowledge of relativity is needed in order to derive the formula describing the phenomenon.

Choose an inertial cartesian frame Σ in which the atom is initially moving with speed u along the $0x$ axis; and choose another inertial cartesian frame Σ' with axes parallel to those of the first and with the $0'x'$ axis sliding along the $0x$ axis with speed u so that in this second frame the atom is initially at rest.

Suppose that in Σ the atom after emitting a photon of frequency ν moves in the xy-plane with velocity $\mathbf{v}$ (x-component v_x) and that the propagation vector of the photon, which because of the conservation of momentum must also lie in the xy-plane, makes an angle θ with the

Ox axis. Denote the corresponding quantities in Σ' by the same symbols with primes affixed.

Define

$$\gamma(w) \equiv \left(1 - \frac{w^2}{c^2}\right)^{-\frac{1}{2}} \tag{1}$$

where w is any speed and c is the speed of light. Let the proper mass of the atom before and after the emission of the photon be M_0 and $M_0 - m_0$ respectively.

The equation expressing the conservation of energy in Σ is

$$M_0 c^2 \gamma(u) = (M_0 - m_0) c^2 \gamma(v) + h\nu \tag{2}$$

h being Planck's constant and that expressing the conservation of the x component of momentum is

$$M_0 u \gamma(u) = (M_0 - m_0) v_x \gamma(v) + \frac{h\nu}{c} \cos\theta . \tag{3}$$

Eliminating $(M_0 - m_0)\gamma(v)$ from these we see that

$$M_0 (u - v_x) \gamma(u) = \frac{h\nu}{c}\left(\cos\theta - \frac{v_x}{c}\right). \tag{4}$$

Since

$$v_x' = -v' \cos\theta' \tag{5}$$

the equation corresponding to (4) in Σ' is

$$M_0 v' = \frac{h\nu'}{c}\left(1 + \frac{v'}{c}\right). \tag{6}$$

By Einstein's composition of velocities theorem we have

$$v_x = (u + v_x')\left(1 + \frac{u v_x'}{c^2}\right)^{-1} . \tag{7}$$

Applying this to the x-component of the velocity of the photon we derive the standard aberration formula

$$c\cos\theta = (u + c\cos\theta')\left(1 + \frac{u\cos\theta'}{c}\right)^{-1} . \tag{8}$$

From (5), (7) and (8) we obtain

(9) $$u - v_x = v'\Lambda$$

and

(10) $$\cos\theta - \frac{v_x}{c} = \left(1 + \frac{v'}{c}\right)\left(1 + \frac{u}{c}\cos\theta'\right)^{-1}\Lambda$$

where

(11) $$\Lambda = \cos\theta'\left(1 - \frac{vu\cos\theta'}{c^2}\right)^{-1}\gamma(u)^{-2}.$$

Substitution from (9) and (10) into (4) yields

(12) $$M_0 v'\gamma(u) = \frac{h\nu}{c}\left(1 + \frac{v'}{c}\right)\left(1 + \frac{u}{c}\cos\theta'\right)^{-1}.$$

Using (6) it thence follows that

(13) $$\nu = \nu'\left(1 + \frac{u}{c}\cos\theta'\right)\gamma(u)$$

which is the formula of the relativistic Doppler effect.

The Archimedeans

The Archimedeans have had yet another successful year, partly due to the hard work put in by last year's committee and partly due to the high standard of the talks delivered. We heard an entertaining talk from Dr. Peter Neumann (Oxford) on "The Mathematical Analysis of 1066 and All That" at the start of the season and half way through the season were startled to see Professor John Nye's calculations on "Glacier Flow". The most enjoyable tea meeting was Dr. T. Körner on "A Pure Mathematician's Revenge–A Dull Talk on Fourier Series". The society's highest traditions were upheld when the president "accidentally" fell in on the punt party and a very pleasant afternoon was spent on the annual ramble when we walked on the Roman road to Linton.

Next year will be somewhat of a new enterprise with the first of the lunchtime meetings which, we hope, will attract more people than the old tea meetings. Among the lunchtime speakers are Dr. Nigel Martin (on "Fu$\eta\eta$iness") and Professor Swinnerton-Dyer. Evening meetings include Dr. R. Berman on "Diamonds" and Professor Northcott on "Absolute Values". More light-hearted activities include the usual punt party and ramble but also include a croquet afternoon for only the second time.

Michael Barnes (*President*)

The Equation $(x^2-1)(y^2-1)=(z^2-1)^2$

by K. SZYMICZEK

In spite of its simplicity the Diophantine equation

(1) $$(x^2 - 1)(y^2 - 1) = (z^2 - 1)^2$$

remains still unsolved that is, all solutions have not been found yet. On the other hand what is known is rather interesting: there is a recursively defined infinite set of non-trivial solutions and moreover three isolated solutions outside this set have been found. It is the purpose of this note to describe the situation in some details and mention some relevant problems proposed by W. Sierpinski.

Our equation has a good many of trivial solutions and we want to exclude them from consideration. First of all we may confine attention to solutions in non-negative integers and because of symmetry in x and y, we may suppose $x \leqslant y$. Now the trivial solutions are the following:

(i) $x = y = z$; (ii) $x = z = 1, y$—arbitrary; (iii) $x = 0, y = z = 1$.

On excluding these we are interested only in solutions satisfying

(2) $$0 < x < z < y,$$

since $0 < x < y$ and (1) imply (2).

Now the first question is whether there are any non-trivial solutions of (1) and it is not difficult to find one such solution: $x = 3, z = 7, y = 17$. Before going on with less trivial questions let us note the following. If x, z, y is a non-trivial solution of (1), i.e. the inequalities (2) are satisfied, then $x^2 - 1, z^2 - 1, y^2 - 1$ form a geometric progression (g.p.). This is very close to a question of W. Sierpinski concerning triangular numbers $t_n = n(n + 1)/2$. There is an easy to notice g.p. formed by three triangular numbers: $t_1 = 1, t_3 = 6, t_8 = 36$ and

W. Sierpinski asked in 1962 whether there are other such g.p. Thus we have to solve the equation $t_a t_b = t_c^2$ and because of $t_n = [(2n + 1)^2 - 1]/8$ this equation is equivalent to (1) with $x = 2a + 1, y = 2b + 1, z = 2c + 1$. Thus the solutions of (1) in odd numbers x, z, y give us triplets of triangular numbers in g.p. and conversely. We notice at once that the solution $x = 3, z = 7, y = 17$ gives $a = 1, c = 3, b = 8$, i.e. t_1, t_3, t_8 form a g.p. as observed above.

It turned out that Sierpinski's question had been considered much earlier and solved in 1914 by A. Gérardin (*Sphinx, Oedipe*, **9** (1914), 75, 146). I found in 1963 (*Publ. Inst. Math.* (*Beograd*), **3** (1963), 139–141) another solution which is simple enough to be reproduced here. W. Sierpinski has proved that if t_n is a square, $t_n = m^2$ say, then the smallest triangular number greater than t_n which is also a square is $t_{3n+4m+1} = (2n + 3m + 1)^2$. Thus $t_1 = 1^2$ gives in turn $t_8 = 6^2$, $t_{49} = 35^2$, $t_{288} = 204^2$, etc. I noticed that if $t_n = m^2$ then the geometric mean of t_n and $t_{3n+4m+1}$ is also a triangular number t_{n+2m} and so $t_n, t_{n+2m}, t_{3n+4m+1}$ form a g.p.
Thus we get infinitely many of such triplets:

$t_1 = 1, t_3 = 6, t_8 = 6^2; t_8, t_{20} = 210, t_{49} = 35^2; t_{49}, t_{119} = 7140,$
$t_{288} = 204^2$; etc.

and these provide an infinite set of non-trivial solutions of (1):

$(x,z,y) = (3,7,17), (17,41,99), (99,239,577)$, etc.

Note that all these solutions are in odd numbers x,z,y and moreover

$z = 2(n + 2m) + 1 = \frac{1}{2}[2(3n + 4m + 1) + 1 - (2n + 1)] = \frac{1}{2}(y - x)$,
that is, all of them satisfy the equation

$$(3) \qquad (x^2 - 1)(y^2 - 1) = [(\tfrac{1}{2}(y - x))^2 - 1]^2.$$

A. Schinzel and W. Sierpinski (*Elem. Math.* **18** (1963), 132–133) have proved that the above set of solutions of (3) is the set of all solutions of (3). This result can be generalised: all solutions of the equation

$$(4) \qquad (x^2 - t^2)(y^2 - t^2) = [(\tfrac{1}{2}(y - x))^2 - t^2]^2$$

in three unknowns x,y,t have been found (cf. the author's note in *Elem. Math.* **22** (1967), 37–38) and H. C. Williams (*Elem. Math.* **25** (1970), 123–125) has found a complete solution of the equation

$$(5) \qquad (x^2 + a)(y^2 + a) = \left[a\left(\frac{y - x}{2a}\right)^2 + b^2\right]^2$$

where a and b are any two given integers.

The equations (3), (4) and (5) are special cases of (1),

$$(x^2 - t^2)(y^2 - t^2) = (z^2 - t^2)^2, \tag{6}$$

$$(x^2 + a)(y^2 + a) = (az^2 + b^2)^2, \tag{7}$$

respectively, and although we know all solutions of (3), (4), (5) we do not know all solutions of (1), (6) and (7).

W. Sierpinski asked whether there are solutions of (1) in even numbers x, z, y satisfying (2) and whether there are non-trivial solutions of (1) other than those satisfying (3). The first question is still unanswered although an attempt to prove that there are no such solutions has been made (cf. W. Zelichowicz, *Prace Mat.* **13** (1969), 113–118). However, as it was pointed out in a review of the paper in the *Mathematical Reviews* (*MR* **40**, # 2604) "an error in the last equation invalidates the result". What is easy to prove is that if $x = 2^\alpha X$, $y = 2^\beta Y$, $z = 2^\gamma Z$, where 2 does not divide XYZ, is a solution of (1) in even numbers, then $\alpha = \beta = \gamma$.

As regards the second question I know three exceptional solutions of (1) that is, those not satisfying (3):

$$(x,z,y) = (4,11,31), (2,13,97), (155,2729,48049). \tag{8}$$

The third solution is of particular interest because its existence shows that there is another triplet of triangular numbers in g.p. namely t_{77}, t_{1364}, t_{24024} which is not included in the previous set of such triplets (neither t_{77} nor t_{24024} is a square). It is perhaps interesting how one can find a solution like this and I want now to show how one can do this. We want to find all triplets of the form $x^2 - 1, z^2 - 1, y^2 - 1$ in g.p. with an integral ratio u. Thus we have to solve the system

$$u(x^2 - 1) = z^2 - 1, \qquad u^2(x^2 - 1) = y^2 - 1. \tag{9}$$

Consider the second equation

$$y^2 - (x^2 - 1)u^2 = 1. \tag{10}$$

For any fixed x this is known to have the following solutions

$$y = y_n(x), \qquad u = u_n(x), \qquad \text{where } y_0 = 1, u_0 = 0 \text{ and}$$

$$y_{n+1} = xy_n + (x^2 - 1)u_n, \qquad u_{n+1} = y_n + xu_n, \qquad n = 0,1, \ldots .$$

Putting in $y_n(x)$ and $u_n(x)$ any integer for x we get a solution of (10).

To get a solution of the system (9) one has to solve the first equation in x and z. This gives us the following sequence of equations

(11) $\qquad z^2 = (x^2 - 1)u_n(x) + 1, \qquad n = 0,1, \ldots .$

The cases $n = 0, 1$ are of no interest, when $n = 2$ we have $u_2(x) = 2x$ and from (11) we get

(12) $\qquad z^2 = 2x(x^2 - 1) + 1.$

Write $X = 2x$, $Z = 2z$ then (12) becomes

(13) $\qquad Z^2 = X^3 - 4X + 4.$

This equation defines an elliptic curve on the (X,Z)-plane. There are two obvious rational points on it: $(X,Z) = (1,-1), (2,2)$. Now the line through two rational points (x_1,z_1) and (x_2,z_2) on the curve (13) meets the curve in a third rational point (x_3,z_3). Define the point $(x_3,-z_3)$ to be the sum of the points (x_1,z_1) and (x_2,z_2) and write $(x_1,z_1) + (x_2,z_2) = (x_3,-z_3)$. If $x_1 \neq x_2$ we can get easily the following expressions for x_3, z_3:

$$x_3 = -x_1 - x_2 + [(z_1 - z_2)/(x_1 - x_2)]^2,$$
$$z_3 = z_1 - (z_1 - z_2)(x_1 - x_3)/(x_1 - x_2).$$

Thus we can add together the two trivial points on (13):

$(1,-1) + (2,2) = (6,-14)$ and furthermore, $(6,-14) + (2,2) = (8,22)$, $(8,22) + (6,-14) = (310,5458)$. Hence we have obtained three new points on (13) and these give us three solutions of (12):

$(x,z) = (3,7), (4,11), (155,2729).$

Taking $y = y_2(x) = 2x^2 - 1$ we get

$(x,z,y) = (3,7,17), (4,11,31), (155,2729,48049).$

These are solutions of the system (9) and so of the equation (1), two last of them being "exceptional". Here a remark is needed. We were very lucky in adding points on the curve (13) since in general the sum of two integral points is a rational (not necessarily integral) point.
Let us consider now the equation (11) for the next values of n. When $n = 3$ we get $u_3(x) = 4x^2 - 1$ and (11) becomes

(14) $\qquad z^2 = 4x^4 - 5x^2 + 2.$

There is an extremely simple way of proving that this equation is insoluble in integers z, $x > 1$. For if $x > 1$ is any integer then $(2x^2 - 2)^2 < 4x^4 - 5x^2 + 2 = (2x^2 - 1)^2 - x^2 + 1 < (2x^2 - 1)^2$

that is, $4x^4 - 5x^2 + 2$ lies between the squares of two consecutive integers and so cannot be a square of an integer.

When $n = 4$, $u_4(x) = 8x^3 - 4x$ and (11) becomes

$$z^2 = 8x^5 - 12x^3 + 4x + 1.$$

It would be a difficult problem to find all integer solutions of this equation but it is easy to find one solution: $x = 2$, $z = 13$. This gives the third of the exceptional solutions (8) of (1).

It is interesting that the clever method of handling (14) can be successfully repeated in the next case when $n = 5$. In fact I can prove by induction that none of the equations

$$z^2 = (x^2 - 1)u_{2n+1}(x) + 1, \qquad n = 1,2, \ldots$$

has a solution in integers z, $x > 1$ and the argument is that for any integer $x > 1$,

$$(y_{n+1}(x) - 1)^2 < (x^2 - 1)u_{2n+1}(x) + 1 < (y_{n+1}(x))^2.$$

Thus it remains to solve the equations (11) for even values of n. By a Siegel's theorem, each of them can have only a finite number of integral solutions, but obviously, this does not imply that the system (9) has only a finite number of solutions.

As we have seen the following questions are still open:

(i) Do there exist infinitely many solutions of the equation (1) which are not solutions of (3)?

(ii) Do there exist non-trivial solutions of (1) in even numbers x,y,z?

Finally, let us mention another question put forward by W. Sierpinski:

(iii) Does there exist a geometric progression formed by four triangular numbers?

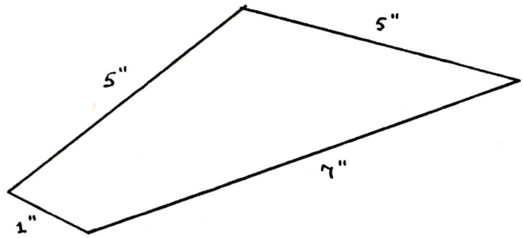
I conjecture the following answers to these questions:

(i) "yes", (ii) "no", (iii) "no".

Geometrical

1. A, B, C, D all lie on a circle with BD as diameter.
AB, BC, CD, DA, BD are all an integral number of inches in length and all different.
What is the shortest length that BD can be?

2. A plane linkage has sides of length 1″, 5″, 5″, 7″ as shown:



What is the largest area it can enclose?

(Solutions on page 54.)

Euleriana

by BERTHA JEFFREYS

In looking through the volume published by the Akademie Verlag, Berlin, in 1959 for the 250th anniversary of Euler's birth, I noticed that W. Blaschke stated that it is not well known that quaternions were given by Euler. The reference given led me to the Euler-Goldbach correspondence, which was carefully edited for the Berlin Academy of Sciences and published in 1965 soon after the 200th anniversary of the death of the "in the history of mathematics often underrated Goldbach" (see for example the remark by Courant and Robbins on p. 30 of *What is Mathematics?*). This volume is in the University Library (P 500.b.156.4) and is more easily handled than the *Opera Omnia* (348.6.b.90.1 – 86). I commend it to anyone who is prepared to cope with its macaronic style, a mixture of German and Latin. The following notes arise from it. In the first I chose 91 for the numerical example because the oldest member of the Faculty, Mr. Cunningham, reached this age on 7 May of this year.

(i) *Did Euler discover quaternions?*

The fundamental result necessary for the theory of quaternions occurs in a letter from Euler to Goldbach of 4 May, 1748. There is a discussion of some formulae that Goldbach has suggested for "transmutationes" of a sum of four squares and he politely remarks that one of them must be wrong, because it would imply that any even number would be a sum of three squares, which is clearly not true for 28 and 60; it was indeed a slip of the pen as appears from the reply. Then comes the important result: "The following theorem can also serve in many cases to determine the four squares of which a number is the sum; if $m = aa + bb + cc + dd$ and $n = pp + qq + rr + ss$, then $mn = A^2 + B^2 + C^2 + D^2$, where

$$(1) \quad \begin{aligned} A &= ap + bq + cr + ds \\ B &= aq - bp - cs + dr \\ C &= ar + bs - cp - dq \\ D &= as - br + cq - dp." \end{aligned}$$

He points out that this can be done in many ways, since the numbers a,b,c,d,p,q,r,s can be taken positive or negative and combined in different orders. It is clear that Euler was concerned here with integers.

The result can be put in quaternion form. Given that

$$i^2 = j^2 = k^2 = -1, \qquad jk = -kj = i, \text{ etc.}$$

we have that

$$A + Bi + Cj + Dk = (a - bi - cj - dk)(p + qi + rj + sk)$$

but I cannot discover that Euler used this notation.

Further in a paper written in 1770 (*Opera Omnia*, Ser. I, Vol. 6, 285-315) entitled "Problema algebraicum ob affectiones prorsus singulares memorabile" Euler uses the result (1) to construct a matrix such that the sum of the squares of the elements in each row and in each column is the same. The use of quaternions is not explicit in this, but it is in a paper by Cayley in 1855 (*Collected Papers*, Vol. 2, 202-215). It may be noted here in parenthesis that the stone over the door of the Garden House Hotel with the inscription recording that it was the home of Professor Cayley from 1864 to 1895 has survived the recent fire.

There is not space for the rather extended general matrices and so, following Euler's example, I give a numerical illustration of his result. In the transformation

$$(2) \quad \begin{aligned} W + Xi + Yj + Zk = (a - bi - cj - dk)&(w - xi - yj - zk) \\ &(p + qi + rj + sk) \end{aligned}$$

put

$$a = b = c = 1, d = 2; \qquad a^2 + b^2 + c^2 + d^2 = 7$$

$$p = -1, q = r = s = 2; \qquad p^2 + q^2 + r^2 + s^2 = 13$$

and we obtain

$$\begin{pmatrix} W \\ X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 7 & 1 & 5 & 4 \\ 5 & 5 & -4 & -5 \\ 1 & -4 & 5 & -7 \\ 4 & -7 & -5 & 1 \end{pmatrix} \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix}$$

With this choice of signs the general matrix is precisely the set of 16 numbers set out by Euler on p. 311 of the 1770 reference given above.

In the numerical example the sum of the squares of the elements in each row or column is 91 (= 7 x 13) and also as Euler puts it the sixteen numbers "rejoice in the property" that the sums of the products from two columns or two rows vanish. The step to a (4 x 4) orthogonal matrix is immediate. Putting $a = p$, $b = q$, $c = r$, $d = s$ in (2) leads to a (3 x 3) orthogonal matrix, which is the object of his paper.

Both Blaschke and B. A. Rozenfel'd in *Ist. mat. issl.* (*Hist. Math. Studies*) **X**, 1957, 392-397, put Euler's results in quaternion form. However, the editor of Euler's works remarks that Euler does not give his derivation; it may indeed have been intuition, using different forms of the expressions in (1) and these are in fact basic to the theory of quaternions.

(ii) Whose, or why, or which, or *what*—was Goldbach's conjecture?
or What's become of Waring?

Goldbach may be described as a polymath or a dilettante according to taste; he certainly carried on a voluminous correspondence and formed lifelong friendships with the mathematicians and scientists of his time. The conjecture occurs in a letter to Euler of 7 June, 1742. He remarks that, when a proposition, originally thought to be true but not proved, has been shown to be false, this can lead to the discovery of new results. As an example of this he mentions Euler's discovery that the Fermat number $2^{2^5} + 1$ is not a prime. He goes on to remark that it would be surprising if all Fermat numbers could be expressed as a sum of squares in one way only and immediately follows this by "hazarding a conjecture" of his own: that if a number is the sum of two primes it is the sum of as many primes as one likes, counting unity as a prime. Lower down the page he illustrates this for 4, 5 and 6 (!) However *in the margin* together with another sentence or two he writes, "It seems, at all events, that any number greater than two is the sum of three prime numbers". In his reply Euler bases a proof of the first of these conjectures on a suggestion previously made to him by Goldbach that any even number can be expressed as the sum of two primes; he remarks that he believes this to be true but cannot prove it. "Das aber ein jeder numerus par eine Summa duorum primorum sei, halte ich für ein ganz gewisses Theorema, ungeacht ich dasselbe nicht demonstrieren kann." *Ten years later* he writes to Goldbach that he has "found among his papers" a suggestion that any number of the form $4a + 2$ is the sum of two primes of the form $4n + 1$ and that he has checked this up to 230 and that for 210 it can be done in nine ways.

It appears that both Euler and Goldbach included 1 in the primes and that the conjecture in its modern form that any even number > 2 is the sum of two primes (excluding 1) cannot be attributed to Goldbach. In fact Descartes had suggested that every number can be expressed as the sum of not more than three primes, but his manuscript was not *published* till 1908.

The conjecture made by Waring (of Magdalene) appears in his *Meditationes algebraicae* (1770) and is simply "Any even number is the sum of two primes, and every odd number is a prime or the sum of three primes &c." The "&c" is tantalising. Apparently he provided no attempt at a proof. Either Descartes or Goldbach must have priority for a suggestion that has provided a great deal of work for later generations. A summary of this is given on p. 106 of the Euler-Goldbach letters.

(iii) *Serendipity.* The "accidental" discovery that $2^{2^5} + 1$ is not a prime.

Euler's discovery that $2^{32} + 1$ is not a prime appears in the *Opera Posthuma*, edited by his great-grandsons, P. H. and N. Fuss. He investigated whether various numbers in the binary scale could be factors of a number of the form $2^n + 1$. His working for $2^{32} + 1$ is long and there are two obvious errors of copying (a 5 for an 8 in two places). The method can be illustrated by taking $1 + 2^3 + 2^5$ as the factor. In the working it is understood that when there are two terms 2^n they are replaced by 2^{n+1} and a dot is placed before the terms 2^n which are no longer to be counted.

Multiplier	Product
1	$1 + .\cancel{2^3} + .2^5$
2^3	$.\cancel{2^3} + .2^6 + .2^8 + .2^4$
2^4	$.2^4 + .2^7 + .2^9 + .2^5 + .2^7 + .2^8 + .2^9 + 2^{10}$

It follows that

$$1 + 2^{10} = (1 + 2^3 + 2^4)(1 + 2^3 + 2^5)$$
$$= 25 \times 41.$$

To follow this, it is necessary to work it out in steps. I have indicated the first of these by deleting the two 2^3's.

When I Went a Rowing

Seven boats A, B, C, D, E, F, G start in that order on the first of n days of bumping races, which are rowed according to the rules below. At the end of the nth day the boats are in reverse order: G, F, E, D, C, B, A.

(i) What is the smallest n for which this is possible?
(ii) Give a possible sequence of events for this n.

Rules:

(1) If boat X bumps boat Y, X and Y immediately drop out of the race. On the next day their starting order is reversed. X can only bump Y if all boats in between have dropped out.
(2) If a boat reaches the end of the course without being involved in a bump it starts in the same position next day.

(Solution on page 54.)

Geometry by Computer

by Professor M. S. LONGUET-HIGGINS

Two years ago Professor Edge[1] issued a challenge to the readers of *Eureka* to prove or disprove the following conjecture.

Suppose we are given a fixed line A in space of three dimensions, and four skew lines B_1, B_2, B_3 and B_4 intersecting A. By a well-known theorem[2] there is just one other line intersecting B_1, B_2, B_3 and B_4, which we may call C_{1234}.

Now given A and five general lines $B_1, \ldots B_5$ intersecting A we get five lines $C_{2345}, C_{1345}, C_{1245}, C_{1235}, C_{1234}$. The theorem of the *double six*[3] says that the five lines $C_{2345}, \ldots C_{1234}$ all intersect the same line, say D_{12345}.

Moreover, given A and *six* general lines $B_1, \ldots B_6$ intersecting A we have six lines $D_{23456}, \ldots D_{12345}$ and by a theorem due to Grace[4] these six lines all intersect the same line E_{123456}. We call this the "Grace line".

The question now is: given A and *seven* intersecting lines $B_1, \ldots B_7$, do the seven Grace lines $E_{234567}, \ldots E_{123456}$ all intersect the same line?

Naturally one would think that they might. But though Grace's paper appeared seventy years ago, no conclusive proof or disproof had been given. Professor Edge adds, "The concensus, if one may describe the opinions of people so few in number as competent to hold one, is that they do not."

This clearly was not good enough. A simple thought occurred to the writer: why not test the conjecture numerically? Any straight line in three dimensions is defined uniquely by six homogeneous coordinates (l,m,n,p,q,r), not all zero, provided they satisfy

$$lp + mq + nr = 0.$$

Any two lines (l,m,n,p,q,r) and (l',m',n',p',q',r') intersect if and only if

$$(lp' + mq' + nr') + (l'p + m'q + n'r) = 0.$$

So we can, in principle, test the conjecture simply by solving a sufficient number of linear equations.

In Grace's day, the labour involved would have made this procedure quite impracticable, but nowadays a high-speed computer can produce the answer in a flash. As Professor Edge afterwards remarked,

"Flectere si nequeo superos, Acheronta movebo."[5]

In short, for the line A I took the z-axis, with line-coordinates $(0,0,1,0,0,0)$. Any other line B intersecting A meets A in a point $(0,0,\zeta)$, and B meets the z-plane in another point $(\xi,\eta,0)$. The six line-coordinates of B are then

$$(\xi, \eta, -\zeta, \eta\zeta, -\zeta\xi, 0).$$

To specify the seven non-intersecting lines $B_1, \ldots B_7$ we have only to take seven triplets of numbers (ξ,η,ζ) such that no two of the ζ's are the same and no two ratios $\xi : \eta$ are equal.

Two calculations were done.[7] In the first, I took sixty-three digits at random from a well-known reference book[6] out of which were formed twenty-one three-digit numbers $\xi_i, \eta_i, \zeta_i, (i = 1, \ldots 7)$. From these, the coordinates of the seven Grace lines $E_{234567}, \ldots E_{123456}$ were calculated, with a double-precision word-length of fourteen decimal places. Along the way, about six decimal places were lost, leaving about eight significant figures to each coordinate.

How does one test whether seven lines have a common transversal? One way is to observe that the coordinates of any *five* lines in general satisfy an equation of the form

$$(Ll + Mm + Nn) + (Pp + Qq + Rr) = 0$$

where L,M,N,P,Q,R are constants. We then say that the lines belong to the *linear complex* with coordinates (L,M,N,P,Q,R). If in particular

$$\text{(A)} \qquad LP + MQ + NR = 0$$

then the five lines all intersect the same line, whose coordinates are (P,Q,R,L,M,N) and we say that the linear complex is *special.*

Out of seven lines we may choose twenty-one sets of five, and when the coordinates of the twenty-one complexes formed by the seven Grace lines were computed they were found to be identical, to nine decimal places. *But* when the left-hand side of (A) was calculated (a relatively simple procedure) it was found to equal about 10^7 times the probable rounding error. (Later the programme was transferred to another machine with a word-length of twenty-nine decimal places and the calculation was verified to twenty-three significant figures.[7])

All the twenty-one linear complexes being virtually identical, we have a cast-iron check on the calculations. But since the condition (A) was not satisfied, the conjecture was shown to be definitely untrue.

Or was it? Could we conceivably have introduced rounding errors greater than we supposed? To eliminate this possibility entirely a second calculation was done in *integers*, or to be more precise, in rational arithmetic, without rounding errors of any kind. This involved the handling of large numbers—up to 10^{60}—for which special sub-routines had to be devised. The results, however were similar: the seven Grace lines all belonged to the same linear complex (with integer coordinates of order 10^{30}), but this complex was not special. Hence there was *no* line intersecting all seven.

So the conjecture is disproved, by the second counter-example, if not the first. Another counter-example, using a complex field of coordinates, has been given independently by Hirschfeld.[8]

On the other hand, we have made a new discovery, namely that the seven Grace lines, though not having a common transversal, do all belong to the same linear complex. No orthodox proof of this has yet been found—a further challenge.

Some intriguing questions arise. Is a numerical proof more, or less, convincing than a logical proof? For, in programming a computer, as every schoolboy knows, mistakes can be made; in a long programme some kind of check is always necessary. If a proposition is found numerically to be *untrue*, the chance of a mistake remains—unless as in the present instance we have a convincing check close to the end. On the other hand if a general proposition is found to be *true* numerically to, say, twenty places of decimals, the chance of an error is slight. In other words, numerical *proof* is more convincing than numerical *disproof*. The paradox is that we have used a (logically) unproved result as a convincing but necessary check on the validity of a (logically) rigorous counter-example.

References

(1) W. L. Edge. Double six. *Eureka*, **33** (1970), 10–12.
(2) H. F. Baker. *Principles of Geometry*, Vol. 3, c.1. Cambridge, 1923.
(3) Ditto, c.4.
(4) J. H. Grace. Circles, spheres and linear complexes. *Proc. Camb. Phil. Soc.* **16** (1898), 153–190.
(5) Virgil, *Aeneid*, Book 7, 1.312.
(6) *London Telephone Directory S-Z*, July 1969, p. 3512.
(7) M. S. Longuet-Higgins. A numerical disproof of a conjecture in projective geometry. *Proc. Roy. Soc. A*, **323** (1971), 443–453.
(8) J. W. P. Hirschfeld. A projective configuration. *Computational Problems in Abstract Algebra.* Pergamon Press (1970), pp. 321–323.

Once Upon a Time

In Dhary, a small principality on a perfectly flat plateau in the Jammanuran mountain range all the roads are straight. In the survey of 1729, the following distances between the principal towns of Ahrens, Bastien, Charves, and Errera were found to be:

	A	*B*	*C*	*D*	*E*
A		2		6	
B	2		8		7
C		8		8	
D	6		8		15
E		7		15	

(All distances in miles)

How far is it from Charves to Errera?

(Solution on page 54.)

A NEW PROOF THAT THE INVARIANT POLYGROUPS ARE ISOMORPHIC TO THE QUASITROPIC SET OF ANTISYMMETRIC HEDROIDS, WITH AN APPLICATION TO THE THEORY OF DYNAMICS IN SPACES OF UNCOUNTABLE DIMENSION.

This proof revolves around the relatively new concept of the reversible quasitropic subcollection (a hedroid is reversible if its Johnson complement is diatonically sub-similar to itself). The crucial result used is that for any hedroid κ

$$\kappa = [\varepsilon, \delta^*]\delta \oplus [\delta, \varepsilon^*]\varepsilon \quad \text{where } \delta, \varepsilon \text{ are reversible}$$

(See K.F.Liu 'New develpoments in hedroid theory' Journal of South Laosian Philosophical Society, Vol. XII pp. 134-288.)

First we consider a special case:

Let $(\mathcal{S}, A, \alpha)$ be an invariant polygroup.

Assume w.l.o.g. $\mathcal{S} \sim [\int_\lambda \mathcal{H}(F(A))\uparrow, \lambda \in \mathcal{K}_\alpha]$

where $\mathcal{K}_\alpha$ is the corresponding isopedric family and F is the Ffomlgh function.

Then for any ε in the reversible quasitropic subcollection

$$(\varepsilon)\alpha^* = \int_\alpha \mathcal{H}(\varepsilon)\uparrow$$

=> $\quad \varepsilon^* = [A, \mathcal{H}(\varepsilon), \alpha]$ using Bernstein's square bracket notation

I.e. $\quad [A, \mathcal{H}(\varepsilon), \alpha] = [A, \mathcal{H}(\alpha), \varepsilon]$

So then by hedroid property

$$[A, \mathcal{H}(\alpha), \varepsilon] \equiv [A][\mathcal{H}(\alpha), \varepsilon] \equiv [A]^*[\mathcal{H}(\alpha^*), \varepsilon]$$

$$\equiv [A^*, \mathcal{H}(\alpha^*), \varepsilon] \equiv [A, \mathcal{H}(\varepsilon^*), \alpha]$$

Thus we have $[\varepsilon, \varepsilon^*] = 1_{\mathcal{S}}$ (which is the n. and s. condition for quasitropic isomorphism).

Now to generalise to non-reversible subcollections:

$\forall \kappa \in B$, B a quasitropic set

$$\kappa = [\varepsilon, \delta^*]\delta \oplus [\delta, \varepsilon^*]\varepsilon \quad \text{for reversible } \delta, \varepsilon.$$

So $\quad (\kappa)\alpha^* = \int_\alpha \mathcal{H}(\kappa)\uparrow$

=> $\quad \kappa^* = [A, \mathcal{H}(\kappa), \alpha]$

$$[\varepsilon, \delta^*]\delta^* \oplus [\delta, \varepsilon^*]\varepsilon^* = [A, \mathcal{H}(\kappa), \alpha]$$

$$[A][\mathcal{H}(\kappa), \alpha] = [A]\{\mathfrak{F}_\alpha([\varepsilon, \delta^*]\mathcal{H}(\delta)) \oplus \mathfrak{F}_\alpha([\delta, \varepsilon^*]\mathcal{H}(\varepsilon))\}$$

Now $\mathfrak{F}_\alpha([\varepsilon, \delta^*]\mathcal{H}(\varepsilon)) = [\mathcal{H}(\varepsilon^*), \alpha][\varepsilon, \delta^*]$

Then by using uniqueness properties (as in Bernstein, 1951) and by variation of the range of ε, δ we get

$$\varepsilon^* = [A, \mathcal{H}(\varepsilon^*), \alpha]$$

$$\delta^* = [A, \mathcal{H}(\delta^*), \alpha]$$

and proceed as in the special case.

Corollary: $[\varepsilon, \delta(*)]$ is a reversible sub-hedroid closure.

We leave the proof to the reader (hint: use Bernstein's sub-hedroid lemma).
(Note the obvious consequences for intactic contrapurence theory.)

To apply the theorem to uncountable dimensioned spaces, we use the well known fact that any complete set of dynamic states can be embedded in an invariant polygroup and hence by the theorem into the quasitropic set of antisymmetric hedroids with generalised quasitropic cardinality.

Example: Consider the explosion of a slow McSandys bomb in an uncountable dimensioned space. We seek to verify the postulate that the fragments of the bomb will each exist in a countable dimensioned subspace and that there will be countably many of them.

Let the state after the explosion be represented by (δ, E, α) where $E \sim$ Expansion value and is (quasi) reversible since bomb idealised (McSandys property).

Then, if K is the corresponding hedroid,

$$K = [\varepsilon, \delta^*]\delta \oplus [\delta, \varepsilon^*]\varepsilon$$

where $\varepsilon \sim [\int(E)]$

and $\delta \sim [\int_R(E)]$ by slowness (McSandys, 1957)

Now by theorem $[\varepsilon, \varepsilon^*] = 1_\delta$ and so

$$[\int(E), \int^*(E)] = 1_\delta$$

$$\begin{aligned} a &= [[\int(E), \int^*(E)]E] = [1_\delta E] \\ &= \int(\mathcal{H}(1_\delta)E\uparrow)\uparrow \\ &= \int(E)\uparrow \mathcal{H}(1_\delta)\uparrow \\ &= \int(E)\uparrow \int\mathcal{H}(1_\delta)\uparrow \end{aligned}$$

But $\int\mathcal{H}(1_\delta)\uparrow = 1$

and so $a = \int(E)\uparrow$ which is countable

Which in fact proves that such a bomb would have no effect.

Readers might like to prove for themselves that the same is not true of a countably infinite collection of such bombs.

B. G. Smith and R. J. Collins

Several Complex Variables

by Professor G. R. ALLAN, *University of Leeds*

The study of *holomorphic* (i.e. *analytic* or *regular*) functions of a single complex variable has long been an established part of the Tripos. By contrast, the study of holomorphic functions of several complex variables has been sadly neglected, not only in Cambridge but in this country generally. This neglect is greatly to be regretted, for the subject stands in the front line of mathematical research and presents scope for the application of a wide range of ideas drawn from analysis, algebra and topology. The present article is written in the hope that some of its readers may be attracted to work in the field. The main centres of activity in the subject are in Europe, the United States, the Soviet Union and Japan but there are signs of an awakening interest in this country also.

This article can only touch on a few topics and suggest some further reading. It is hoped that a little of the appeal of the subject may be conveyed.

Firstly, what *is* a holomorphic function of several complex variables? As in the case of a single variable, there are several alternative definitions. Suppose that U is an open subset of $\mathbf{C}^n$ and that f is a complex-valued function on U. Then f is said to be *holomorphic* on U if it is complex-differentiable at each point of U; thus for each $z = (z_1, \ldots, z_n)$ in U there are complex numbers $\alpha_1, \ldots, \alpha_n$ such that

$$f(z+h) = f(z) + \sum_{k=1}^{n} \alpha_k h_k + o(|h|),$$

as $|h| \to 0$, where $h = (h_1, \ldots, h_n) \in \mathbf{C}^n$ and $|h|$ denotes the Euclidean norm of h. Equivalently we may say that f is differentiable as a function of the $2n$ underlying real variables x_k, y_k $(k = 1, \ldots, n)$, where $z_k = x_k + iy_k$, and that f satisfies the Cauchy-Riemann equations

$$\frac{\partial f}{\partial x_k} = -i \frac{\partial f}{\partial y_k} \qquad (k = 1, \ldots, n).$$

It is again equivalent to require that f have a convergent Taylor expansion (in n variables of course) about each point of U.

A remarkable classical result in this area is the theorem of Hartogs

(1906) which states that for f to be holomorphic on U it is sufficient (and trivially necessary) that f be holomorphic in each variable separately, or, in other words, that the n complex partial derivatives $\partial f/\partial z_k$ exist throughout U. This result is of course in marked contrast to the situation existing for differentiability of functions of several *real* variables.

The first hint of a significant departure from analogy with the one variable case comes with the following result, also due to Hartogs (1909). Again let U be an open subset of $\mathbf{C}^n$ (some $n > 1$), let $a \in U$ and let f be holomorphic on $U \backslash \{a\}$; then there is a holomorphic extension of f to the whole of U. The contrast with the case $n = 1$ is evident.

The domain $D = \{z \in \mathbf{C}^n : |z_k| < 1 \ (k = 1, \ldots, n)\}$ has the property that there is a holomorphic function f defined on it which can not be extended to be holomorphic on any larger domain; such a domain is called a domain of holomorphy. By contrast, when $n > 1$, the domain $D_0 = D \backslash \{0\}$ is not a domain of holomorphy, for, by the result mentioned in the last paragraph, every holomorphic function on D_0 can be extended to D. The problem of characterising domains of holomorphy in some reasonable way is not easy. It was solved by Oka (1953) in terms of the concept of pseudo-convexity, which will not be discussed here. (We note that in case $n = 1$ the solution is easy: every subdomain of $\mathbf{C}$ is a domain of holomorphy.)

A good account of the elementary theory—that is to say the part not involving more sophisticated algebraic machinery—may be found in R. Narasimhan: *Several Complex Variables* (Chicago Lectures in Mathematics, 1971). This covers all the topics so far mentioned in this article. The reader who wishes to go further should certainly consult the stimulating notes by Lipman Bers: *Introduction to Several Complex Variables* (Courant Institute, New York, 1964). It may also be useful to mention the enjoyable notes of R. C. Gunning: *Lectures on Riemann Surfaces*, since, although these deal with a single complex variable, they introduce the algebraic machinery of sheaf cohomology theory in a technically simpler case and thus serve as a very useful introduction to these ideas, quite apart from their inherent interest.

It's a Knockout!

A knockout competition starts with 128 competitors and 16 of them are seeded so that no two of these may meet until the fourth round.

Each seeded competitor has a ranking number between 1 and 16. A seeding upset occurs if a seeded player is beaten by an unseeded one or by a seeded competitor who is ranked lower.

(i) What is the smallest possible number of matches involving at least one seeded player?
(ii) What is the greatest number of matches involving at least one seeded player?
(iii) What is the greatest possible number of seeding upsets in the competition?

(Solution on page 54.)

Where Did I Leave That Arsenic? or, Sequential Search Procedures

by Professor P. WHITTLE

A search problem can have many variants. For one of the commonest, consider the problem of looking for a bicycle in Cambridge (a *particular* bicycle), which is considered lost rather than stolen or strayed, and so may be presumed stationary. One's initial feeling is that some places are more likely than others: the Arts School courtyard, the Mill Pond, and the roof of King's Chapel probably form a sequence of decreasing probability. On the other hand, in examining some sites one gets at least a partial view of others. The roof of King's Chapel may be implausible in itself, but the panorama of Cambridge it affords must include some view, if fragmentary and distant, of Cambridge's bicycles. Yet again, however, the time and labour of the ascent must be taken into account.

Suppose we discretise the situation in both space and time by assuming that the missing bicycle could be at one of a number of sites, indexed $i = 1,2, \ldots, m$, and that one can examine a site for unit time (a *scan*), and then decide either to inspect there further or to move on to another site. Let P_i be the probability (conditional on current information) that the bicycle is at site i; let P_{ji} be the probability that, if at site i and scanned from site j it remains undetected. If detected, that is the end of the matter. If undetected, then $P = \{P_i\}$ suffers the transformation

(1) $$P_i \to T_j P_i = \frac{P_{ji} P_i}{\sum_k P_{jk} P_k}$$

Suppose the cost of scanning from site k immediately after having scanned from site j to be c_{jk}; this will measure both the cost of movement and the cost of a further scan. The aim is to minimise the expected total cost up to the instant of detection. An inductive proof shows that this expected further cost, starting from a posterior distribution P, and a site j, is a function of j and P alone, $F_j(P)$ say. This function satisfies the dynamic programming relation

(2) $$F_j(P) = \min_k \left[c_{jk} + (\sum_i P_{ki} P_i) F_k(T_k P)\right].$$

A further inductive argument shows that, if c_{jk} is replaced by $c_{jk} \sum P_i$ then the definition of $F_j(P)$ can be consistently extended to cases where $\sum P_i \neq 1$ by assuming F homogeneous of degree one in P; relation (2) then simplifies to

(3) $$F_j(P) = \min_k \left[c_{jk} \sum P_i + F_k(\{P_{ki} P_i\})\right]$$

The solution of the optimal search problem must be implicit in this relatively simple relation, but this solution is evident only in the most elementary cases.

A plausible asymptotic state, possible with certain site geometries, is that of dynamic equilibrium, in which the searcher moves in a cyclic pattern, and $\{P_i\}$ as seen from a system of co-ordinates moving with the searcher, changes only by a factor as time goes on, and the search remains fruitless. To take the simplest case, suppose that the m sites are spaced equidistantly around the circumference of a circle, and that the searcher moves one step around the circle at each instant in the direction of increasing j (j then to be reduced mod m).

Suppose the search space homogeneous in that P_{ji} is a function of "distance" $i - j$ alone, say a_{i-j}. Suppose further, that if the searcher is at j, then $P_i \propto \pi_{i-j}$ where π does not change in time: this is the assumption of equilibrium in co-ordinates centred on the searcher. Requiring this invariance under the transformation (1) and a step $j \to j + 1$ we deduce that

(4) $$a_{i-j} P_{i-j} = \lambda \pi_{i-j-1}$$

(For, $v = \bar{u}$, $P(v) = \overline{P(u)}$.) If $\delta \neq 0$ and $\Delta = 0$, then all the roots are real but not distinct.

Notice that, when applied to the equation $x^3 + px + q = 0$, formulae (2) and (7) reduce to the well-known Cardan's formula. (In this case $P(u)/P(v)$ equals u/v.)

To conclude, I suggest the reader to try to use substitution (3) to transform the general equation of the fourth degree into a biquadratic equation.

The Mathematical Association

150 Friar Street, Reading, Berkshire, RG1 1HE

President: Mr. C. T. DALTRY, B.Sc.

The Mathematical Association, which was founded in 1871 as the Association for the Improvement of Geometrical Teaching, aims not only at the promotion of its original object but at bringing within its purview all branches of elementary mathematics.

The Association publishes two journals, *The Mathematical Gazette* and *Mathematics in School.* The former, published four times a year, deals with mathematical topics of general interest whereas the latter is specifically designed for schools. The present editor of *The Mathematical Gazette* is Mr. D. A. Quadling.

At the moment of writing the subscription is £5 (both journals), or £3.60 (*The Mathematical Gazette* only), per annum. The subscription for students is £1.

The Burnside Problem

by IAN STEWART, *University of Warwick*

In 1902 W. Burnside[1,2] posed a problem which is nowadays formulated in three different ways:

1. *Strong Burnside Problem*
   Is every periodic group locally finite?
2. *Burnside Problem*
   Is every group of exponent n (n an integer) locally finite?

3. *Restricted Burnside Problem*

Is the order of a *finite* m-generator group of exponent n bounded in terms of m and n?

(A group is *periodic* if every element has finite order. It is *locally finite* if every finite subset is contained in a finite subgroup. The *exponent* is the lcm of the orders of the elements. An *m-generator* group is one which can be generated by m elements.)

It is only in comparatively recent times that any of these problems have been (even partially) solved. Burnside himself solved (2) when $n = 2$ or 3.[2] The case $n = 2$ is trivial, for any group satisfying $x^2 = 1$ for all elements x must be abelian. For groups of exponent 3 his proof runs roughly as follows:

Let G be a group of exponent 3 having m generators. We show by induction on m that G is finite. When $m = 0$, 1 there is no difficulty.

Now we take any element g of G and any conjugate $x^{-1}gx$. Some simple calculations inside the group generated by g and x shows that g and $x^{-1}gx$ commute. Hence the normal closure (smallest normal subgroup containing) of g in G is abelian. Modulo this G has $m - 1$ generators and is of exponent 3. By induction G is soluble. By another induction G is finite.

Problem (2) can be restated in purely combinatorial form (which may account for its popularity—when in doubt, calculate!). Let $B_m(n)$ be the group generated by m elements $x_1, \ldots, x_m$ subject to the relations $w^n = 1$ for every product w of powers of the x_i. Problem (2) asks whether $B_m(n)$ is always finite; and problem (3) asks whether it has a normal subgroup of finite index such that there is no smaller normal subgroup of finite index.

Levi and Van der Waerden[12] polished up Burnside's result for $n = 3$ by finding the order of B_m (3)—it is

$$m + \binom{m}{2} + \binom{m}{3}.$$

Sanov[16] gave an affirmative answer for $n = 4$ (though the order of the group is not known) and M. Hall[4,5,6] did likewise for $n = 6$. The order of B_m (6) is

$$2^a \cdot 3^{b+\binom{b}{2}+\binom{b}{3}}$$

where $a = 1 + (m - 1)\, 3^{m+\binom{m}{2}+\binom{m}{3}}$

$b = 1 + (m - 1)\, 2^m.$

which follows (once finiteness is established) from work of P. Hall and

G. Higman[7] giving, among other things, various reductions of the Burnside Problem. The Hall-Higman paper is essentially a study of modular representations, and has been the basis of many subsequent investigations in group theory (as we shall see later).

Higman[9] also solved the restricted Burnside problem for $n = 5$ (any m). His methods involved transforming the problem to one in Lie rings.

A *Lie ring L* is an abelian group on which is defined a multiplication $[a,b]$ which distributes over addition, and satisfies

$$[a,a] = 0$$

$$[[a,b]c] + [[b,c]a] + [[c,a]b] = 0.$$

(Examples can be obtained by starting with an associative ring and defining $[a,b] = ab - ba$.) There is a way of turning a group into a Lie ring, based on making the group commutator $x^{-1}y^{-1}xy$ play the part of $[x,y]$. Since the above axioms do not hold exactly for the group commutator it is necessary to modify matters somewhat. It turns out that if the group has prime exponent p then L is a vector space over a field of p elements and satisfies the condition

$$[\ldots[xy]y]\ldots y] = 0$$

where there are $p-1$ factors y. (This is the $(p-1)$th *Engel condition*.) To settle (3) affirmatively when n is prime it suffices to prove that a finitely generated Lie ring which is a vector space over a field with p elements and satisfies the $(p-1)$th Engel condition is finite dimensional (as a vector space). This Higman did for $p = 5$.

Then in 1959 Kostrikin (having already done $p = 7$) proved[11] the above statement in full generality (for primes). This is a difficult task, involving very complicated calculations and cunning inductions. Thus (3) was answered affirmatively for $n = p$, any prime. Using results of Hall and Higman the problem also has an affirmative answer for $n = 4p$ or pq where p, q are prime; and it has recently been proved for $n = 30$ by Mazurov.[13]

Also in 1959 Novikov[14] claimed to have answered (2) *negatively* for $n \geqslant 72$. Several years passed, without a proof emerging. Adyan, a student of Novikov, had found an error (or several) and Novikov and Adyan were working on the problem of putting the errors right. Their proof, over 300 pages long, appeared in several sections during 1968[15] but with one difference: they proved that (3) had negative answer for *n odd and greater than 4381.* One intriguing consequence is that there are values of n for which (2) has negative answer but (3) affirmative.

An independent proof of a similar theorem has recently been found by J. L. Britton.

We have all this while neglected problem (1). The answer has for some time been known to be "yes" for groups of matrices over a field. But in 1964 Golod and Šafarevič produced a beautiful example see (8) of a periodic group which is not locally finite; furthermore the proof is extremely simple (as compared with the marathon efforts inspired by the other two problems).

"Spinoff"

Faced with all the effort which has been expended, it is worth deciding what has really been achieved.

As regards direct answers to (1), (2), or (3) affirmative answers are more helpful than negative ones; which means that most of the effort has been expended in closing off dead ends. Were the answers to the three questions all that had been achieved everything would probably have been a waste of time. But as with many tricky problems, the final solution is less important than the methods by which it is solved.

The work of Golod and Šafarevič has also been applied to two other outstanding problems. They have settled negatively the *Kuroš problem* (is every algebraic algebra locally finite) and constructed an infinite class field tower (carried by the field $Q\sqrt{-3.5.7.11.13.19}$). And applications of their method are by no means exhausted.

The ideas of Novikov-Adyan would seem to be useful in many situations where a group is given by generators and relations. They have shown that for the values of n considered by them $B_m(n)$ has no infinite abelian subgroup; which answers a famous question of Schmidt (does every infinite group possess an infinite abelian subgroup?); Adyan has shown that there exists a variety of groups which has no finite basis for its laws (this has also been proved independently and more simply by Olšanskii and (still more simply) Vaughan-Lee). This was one of the central problems in the study of group varieties, now a flourishing branch of group theory.

The Hall-Higman theorem has perhaps had the greatest repercussions. It was the basis for much of the current work in finite simple (and other) groups. Thompson's first proof of the nilpotency of the Frobenius kernel of a Frobenius group depended on it (via a theorem about fixed-point free automorphisms); the ideas were used in Feit-Thompson's odd-order paper,[3] which disposed of another problem of Burnside: is every odd-order group soluble? Most of the recent progress in classifying simple groups is rooted in the odd-order paper.

of Analysis II, the second year course on Lebesgue measure and a good deal of the Part II courses which deal with L^p spaces. This book makes quick and clear reading, in the informal style of a lecture course. The author's approach throughout is in terms of metric spaces and full use is made of concepts such as connectedness, compactness and completeness, etc; yet despite the greater generality he loses none of the simplicity of an approach dealing only in $\mathbf{R}^n$ and using strictly "non-topological" concepts. In fact, some topics are tackled more simply from this view-point. He also covers some very elegant theorems, which, although not included in most courses at this level, are necessary for the student to gain a full understanding of the subject. Unfortunately the approach to Lebesgue integration is somewhat different to that adopted in the 1B course, but this aside, the book provides good background knowledge.

T. P. Hynes

***Excursions in Geometry* by C. Stanley Ogilvy.**
(Oxford University Press)

This is certainly a book for the enthusiastic amateur. The author brings you through theorems on harmonic division, the Apollonius circle, and inversion geometry to a discussion of projective geometry, leaving much of the easier work to the reader. The chapters on insoluble problems of antiquity and three unsolved problems of modern geometry are particularly interesting, mathematically as well as historically.

For those of us who would like to take up geometry again as a hobby the book provides a lucid and readable account of some of the more interesting problems in classical geometry.

Richard Clayton

Van Nostrand Reinhold Mathematical Studies:
***Topological Dynamics and Ordinary Differential Equations* by G. R. Sell.**
***Compact Non-self-adjoint Operators* by J. R. Ringrose.**
***Lectures on Von Neumann Algebras* by D. M. Topping.**

The Van Nostrand Reinhold Mathematical Studies series aims at providing quick introductions to advanced topics and as such is designed mainly for people with a reasonable amount of mathematical experience and background knowledge. Each of the books is written by an expert in the field; the reader with no previous specialised knowledge is brought to the stage where he can understand and appreciate recent developments and some of the open research problems in the particular area in question.

Professor Sell's book begins with a brief review of the theory of uniform spaces, thereby laying down the setting for the rest of the book. There follows an account of the basic properties of dynamical systems. Definitions come fairly thick and fast here but they are given time to sink in during the chapter which follows on examples of flows; a pleasing feature here is that the examples are drawn from a wide range of topics including Markov processes and measurable functions as well as ordinary differential equations. The next chapter is devoted to showing how flows arise in the study of non-autonomous differential equations; in particular the crucial notion of the limiting equations is introduced. There follow chapters on almost periodic functions, recurrent motions and almost periodic motions, and the structure of ω-limit sets; the main purpose of these is to prepare the way for the applications to differential equations which come next. The discussion is centred on questions of stability and existence of periodic and almost periodic solutions. It is here that the limiting equations play an essential role. The final part of the book deals with invariant measures, ergodic theory and applications of the methods developed earlier to integral equations.

On the whole, the book seems to succeed in bringing the reader to the point where he can understand the abstract theory and the applications to ordinary differential equations and integral equations. He is left to wonder for himself whether the theory and extensions of it could be fruitful in other contexts, for example probability or perhaps even partial differential equations.

The theory of compact non-self-adjoint operators on a Hilbert space has progressed considerably over the past fifteen years. Professor Ringrose in his book attempts to describe some of the more important recent developments in as concise a form as possible. The book begins with a fairly lengthy introduction much of which can be bypassed by the more knowledgeable reader. The next chapter describes the von Neumann-Schatten classes of operators on a Hilbert space **H**; it is shown that these consist of compact operators and form two-sided ideals in **B(H)**, the algebra of all bounded linear operators on **H**. The next chapter develops a Fredholm theory for equations of the form $x - \lambda Tx = y$, where T lies in the trace class of operators on **H**, and $x,y \in \mathbf{H}$. There follows a discussion of quasi-nilpotent operators in a von Neumann-Schatten class and the chapter concludes with some applications to completeness results for the systems of principal vectors of certain non-self-adjoint operators. The concluding chapter contains an account of some recent work of the Russian school on the representation of a compact Hilbert space operator as a "superdiagonal integral".

Professor Topping's is intended to give a brief and hence necessarily incomplete introduction to the theory of von Neumann algebras. Both the algebraic and geometric flavours of the subject are introduced early, the former via the double commutant theorem and the latter via some results on projections. The classification of von Neumann algebras by means of the projections in them is introduced and is followed by a detailed account of some of the type I theory. The author then describes some general structure theory and some topological properties of *-isomorphisms before considering the special case when the underlying Hilbert space is separable. The book concludes with chapters on generators and hyperfinite algebras.

Each of the books is based on a course given to graduate students. The material is presented in a fairly raw state, but this is more than made up for by the fact that the books contain in an intelligible form accounts of important topics many of which could hitherto be found only in research papers. Indeed, the whole Van Nostrand Reinhold Mathematical Studies series must be considered by researchers young and old a very significant addition to mathematical literature.

M. Pemberton

A Guide to Undergraduate Projective Geometry **by A. F. Horadam. (Pergamon Press)**

This is an ambitious book. To quote the jacket, "An attempt is made to balance the classical approach to the subject with the most recent research". To my mind the attempt is not totally successful. Certainly the recent research is in evidence, but the classical approach is not immediately apparent.

The approach seems to me to confuse two distinct functions of a maths book, and in doing so to achieve neither. While rigorous, the treatment is not designed to make reference easy, and the important results are not given sufficient prominence. For a textbook, the ground covered is too wide and the coverage not of the kind required.

On the other hand, the material is not of a nature to make casual reading easy. Certainly, for the mathematician who wants general information about the subject, this book could be useful, but it is hardly light bedside reading.

P. G. Williams

Computational Problems in Abstract Algebra
edited by John Leach. (Pergamon Press)

This book is a collection of papers presented at an Oxford conference in 1967. It is unfortunate that it could not have been published until now; however, it is one of the most up-to-date summaries of the applications of computing to this field presently available.

The subject matter can be broadly divided into two categories—group theory and the rest. In the first category many of the applications are obvious—the algorithmic enumeration of all the possibilities with which one is concerned (in the case of finite groups and subgroups of finite index), and, in general, the manipulation of symbols under well-defined rules. Particularly interesting are two papers on the application of computing to the Burnside problem where the described construction of an algorithm for $L(p,m,n)$ may well provide greater insight.

In the second category the use of computers in alleviating the drudgery of elimination in problems for which step-wise procedures can be devised is motivation for the tackling of problems which otherwise would probably not be attempted. There is included a paper by our own John Conway on the enumeration of knots—the use of computing in this and similar fields is apparent. There is also considered the possibility of dealing with infinite problems by their reduction to finite ones (as in the paper on Galois theory by W. D. Maurer).

The book would be of great use to any researcher in algebra considering using computing to solve an otherwise tedious problem. It is however too expensive to be considered by the majority of general readers. Nevertheless, any algebraist not already aware of the application of computing to his field ought to be made so, and thus this work ought to be found in all pure mathematical libraries.

B. G. Smith

Introduction to Computer Programming **by D. I. Cutler.**
(Prentice-Hall)

This book should interest budding mathematicians from the fourth form upwards. After an introductory section on the evolution of computers and their applications, it expounds various number systems (binary, octal, hexadecimal) in a way I feel sure could be clearly understood by all but the most obtuse. After chapters on data representation and flow diagramming (a useful concept, easily picked up) the book introduces the mythical EX-1 computer, a paragon of standardisation. "Mr. Control" and a series of cartoon diagrams lead you through a small program executed by EX-1. The arithmetical operations are gone into in detail, followed by programming techniques and finally input-output analysis; a somewhat unconventional order.

There is a chapter explaining higher level languages using TRIVIAL (Trusty Reliable Ingenius Version of the International Algebraic Language) as well as chapters on typical modern giant computers and programming systems.

Patronising, in the usual American manner, it nevertheless provides a clear machine-invariant introduction to computer software and programming techniques.

C. J. Slinn

S.M.P. Further Mathematics Series. (C.U.P.)

II Vectors and Mechanics.

An extremely well-written book with a modern approach, intended primarily for the student with only an O Level knowledge of maths. Stress is laid on the applications of derived formulae; in particular, the obscure type of question traditionally set is replaced by a more relevant, and consequently more interesting, one. There are plenty of worked examples and exercises—all with solutions, including those involving a diagram. Vector notation is used throughout, and a vital summary of formulae and notation is included for easy reference.

This is the sort of book that the student can work from on his own, with only a little guidance from the teacher. However, in its present paper-back form, the binding would not survive constant use although it does make it a very cheap book at a pound.

IV Extensions of Calculus.

This book is of an equally high standard but of a slightly more advanced level, giving a good foundation to further study at University. It includes a detailed discussion of linear transformations with work on conformal mapping and Lorentz transformations; also an excellent introduction to the relevance and manipulation of partial derivatives, with main emphasis on the Jacobian and its use in connection with multiple integrals.

Janet Haig

***Solving Problems in Maths: Statistics II* by J. Aitchison.**
(Oliver and Boyd)

Whereas *Statistics I* dealt with the analysis of independent experiments this book is concerned with dependent events. After a description of dependence in probability theory, Professor Aitchison considers inference and decision making, regression analysis, least squares estimation, tests of association and sequential analysis. The inference is considered from a Bayesian point of view. The section on regression analysis is particularly well done, with some interesting examples. In fact, most of the examples in the book are very well chosen, with some having just the right air of whimsicality ("I am offered what could be a genuine Monet . . . ."; "In police investigations into the source of anonymous letters . . . ."). The worked examples are very useful but as is only natural in a book of this kind, there is very little theory and it would be better to use this as a companion text in mathematics courses. An index would undoubtedly have been useful.

I. S. Wilson

Solutions to Problems

(The editor would like to thank the compilers of this year's problems drive, Patrick Phair and Clifford Cocks.)

An Alphametric

$P = 0$ $T = 1$ $R = 2$ $I = 4$ $A = 6$ $S = 8$ $H = 9$
either $L = 3$ $Y = 5$ $E = 7$
or $E = 3$ $L = 5$ $Y = 7$.

Two Problems

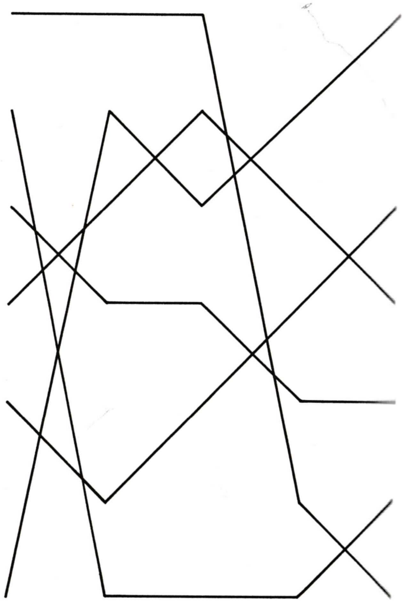
1. (A) 4p. (B) 5/9.
2. If n divides $S(n)$ then $S(n)$ divides $S(S(n))$, but 3 divides $S(3)$.

Geometrical

1. 65″.
2. 16 square inches. (Maximum area when linkage is cyclic.)

When I Went a Rowing

4 days is the minimum, e.g.



Once Upon a Time

13 miles.

It's a Knockout!

(i) 16.
(ii) 63.
(iii) 16.

Printed in Great Britain by
William Clowes & Sons Limited
London, Colchester and Beccles