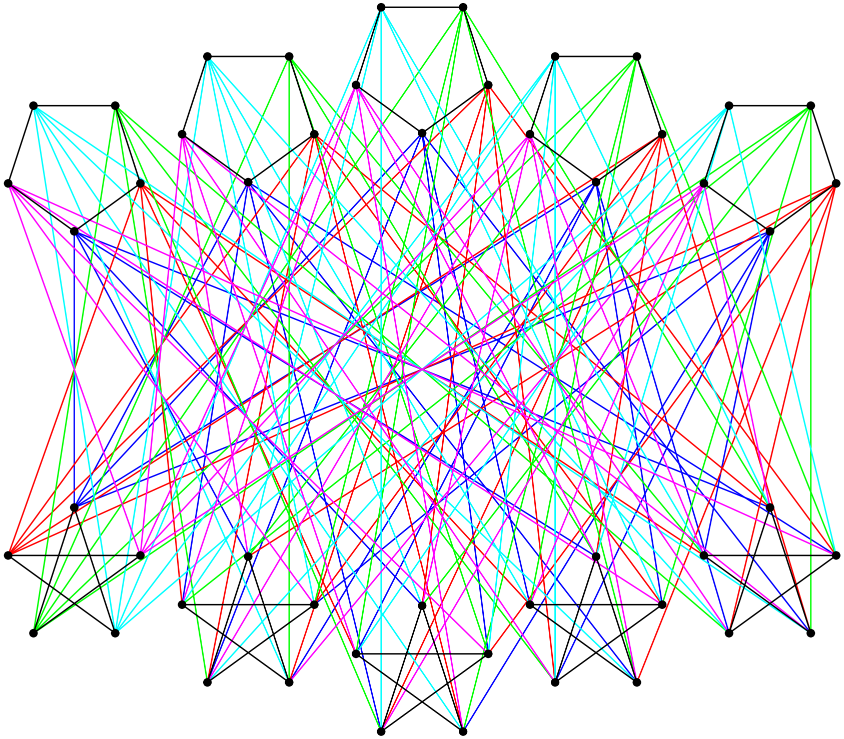
*

ISSN 1350-8539

M500 276



The M500 Society and Officers

The M500 Society is a mathematical society for students, staff and friends of the Open University. By publishing M500 and by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching. Web address: m500.org.uk.

The magazine M500 is published by the M500 Society six times a year. It provides a forum for its readers' mathematical interests. Neither the editors nor the Open University necessarily agree with the contents.

The Revision Weekend is a residential Friday to Sunday event providing revision and examination preparation for both undergraduate and postgraduate students. For details, please go to the Society's web site.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details, please go to the Society's web site.

Advice to authors We welcome contributions to M500 on virtually anything related to mathematics and at any level from trivia to serious research. Please send material for publication to the Editor, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation. For more information, go to m500.org.uk/magazine/ from where a LaTeX template may be downloaded.

M500 Society Committee – call for applications

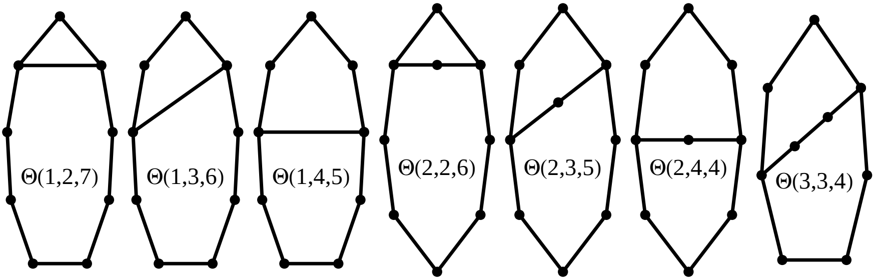
The M500 committee invites applications from members to join the Committee. Please apply to Secretary of the M500 Society not later than 1st October 2017.

Solution 265.6 – Triples

> Show that if n is a positive integer, the number of integer triples (a, b, c), where $1 \le a \le b \le c$ and $a+b+c = n$, is $\lfloor n^2/12+1/2 \rfloor$.

Tony Forbes

A *theta graph*, $\Theta(a, b, c)$, consists of three paths of lengths a, b and c, $a \le b \le c$, $b \ne 1$, that have common end-points but are otherwise disjoint. Looking at the sixth example in the illustration, $\Theta(2, 4, 4)$, you can probably guess why they are so called. And I expect you can remodel the others slightly to conform to the true shape of the said Greek letter.



The seven theta graphs with ten edges

Anybody who studies these things will inevitably want the answers to two questions.

(i) How many theta graphs have n edges?

(ii) How many theta graphs with n edges are bipartite?

Recall that *bipartite* means the vertices can be partitioned into two sets A and B such that every edge joins a vertex in A to a vertex in B.

For positive integer n, let us write $p_k(n)$, $p_k^{\text{even}}(n)$ and $p_k^{\text{odd}}(n)$ for the number of partitions of n into k positive integers, k positive even integers and k positive odd integers respectively. Thus, for example, $p_3(10) = 8$, $p_3^{\text{even}}(10) = 2$ ({2,2,6}, {2,4,4}) and $p_3^{\text{odd}}(11) = 4$ ({1,1,9}, {1,3,7}, {1,5,5}, {3,3,5}). So we want to show that the expression in the statement of Problem 265.6 is equal to $p_3(n)$. Also, in connection with question (ii) concerning bipartite theta graphs, we are interested in obtaining similar formulæ for $p_3^{\text{even}}(n)$ and $p_3^{\text{odd}}(n)$.

For $n \ge 5$, every partition $\{a, b, c\}$ except $\{1, 1, n-2\}$ corresponds to a theta graph $\Theta(a, b, c)$, and conversely; therefore the answer to question

(i) is $p_3(n) - 1$. And since $\Theta(a, b, c)$ is bipartite iff $a \equiv b \equiv c \pmod 2$, the answer to question (ii) is either $p_3^{\text{even}}(n)$ or $p_3^{\text{odd}}(n) - 1$, depending on the parity of n. A theta graph must have at least five edges.

We now proceed to obtain

$$p_3(n) \;=\; \left\lfloor \frac{n^2}{12} + \frac{1}{2} \right\rfloor, \tag{1}$$

which is just $n^2/12$ rounded to an integer. Recall the well-known formula

$$p_k(n) \;=\; p_{k-1}(n-1) + p_k(n-k), \quad n \geq 4, \tag{2}$$

which can be derived by splitting the partitions of n into two types. The first term on the right of (2) counts the partitions that contain a 1, and second term counts those that don't.

If there is a way of showing that (1) is obvious, I am unaware of it. So we resort to a proof by induction—worked out by Carrie Rutherford and myself whilst taking dinner at a fashionable restaurant somewhere in London. The reader can verify (1) for $n = 1, 2, \ldots, 6$. Suppose (1) holds for some positive integer n and consider $n+6$. Using (2) and observing that $p_2(m) = \lfloor m/2 \rfloor$, we have

$$\begin{aligned} p_3(n+6) \;&=\; \left\lfloor \frac{n+5}{2} \right\rfloor + p_3(n+3) \;=\; \left\lfloor \frac{n+5}{2} \right\rfloor + \left\lfloor \frac{n+2}{2} \right\rfloor + p_3(n) \\ &=\; 3 + \left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + p_3(n) \;=\; n + 3 + \left\lfloor \frac{n^2}{12} + \frac{1}{2} \right\rfloor \\ &=\; \left\lfloor \frac{(n+6)^2}{12} + \frac{1}{2} \right\rfloor, \end{aligned}$$

and hence (1) holds for all positive integers n.

For even n, $p_k^{\text{even}}(n)$ is the same as $p_k(n/2)$, got by halving each part. Therefore

$$p_3^{\text{even}}(n) \;=\; \begin{cases} p_3\left(\dfrac{n}{2}\right) \;=\; \left\lfloor \dfrac{n^2}{48} + \dfrac{1}{2} \right\rfloor, & n \text{ even}, \\ 0, & n \text{ odd}. \end{cases} \tag{3}$$

For odd partitions, there is an equality very similar to (3):

$$p_3^{\text{odd}}(n) \;=\; \begin{cases} \left\lfloor \dfrac{n^2}{48} + \dfrac{n}{8} + \dfrac{1}{2} \right\rfloor, & n \text{ odd}, \\ 0, & n \text{ even}. \end{cases} \tag{4}$$

Assume n is odd and positive. By adding 1 to each part and then halving the parts, we see that

$$p_3^{\text{odd}}(n) \;=\; p_3^{\text{even}}(n+3) \;=\; p_3\left(\frac{n+3}{2}\right).$$

So

$$p_3^{\text{odd}}(n) \;=\; \left\lfloor \frac{(n+3)^2}{48} + \frac{1}{2} \right\rfloor \;=\; \left\lfloor \frac{n^2}{48} + \frac{n}{8} + \frac{3}{16} + \frac{1}{2} \right\rfloor,$$

which is exactly like (4) except for that annoying fraction, 3/16. However, and somewhat surprisingly (at least to me), it can be ignored. To confirm this claim we will prove

$$\left\lfloor \frac{n^2}{48} + \frac{n}{8} + \frac{3}{16} + \frac{1}{2} \right\rfloor \;=\; \left\lfloor \frac{n^2}{48} + \frac{n}{8} + \frac{1}{2} \right\rfloor, \quad n \text{ odd}, \tag{5}$$

and again we use induction. Verify (5) for $n = 1, 3, 5, \ldots, 23$. Assume (5) for some positive odd n and consider $n + 24$, which is also odd. Then

$$\begin{aligned} \left\lfloor \frac{(n+24)^2}{48} + \frac{n+24}{8} + \frac{3}{16} + \frac{1}{2} \right\rfloor \;&=\; n + 15 + \left\lfloor \frac{n^2}{48} + \frac{n}{8} + \frac{3}{16} + \frac{1}{2} \right\rfloor \\ &=\; n + 15 + \left\lfloor \frac{n^2}{48} + \frac{n}{8} + \frac{1}{2} \right\rfloor \;=\; \left\lfloor \frac{(n+24)^2}{48} + \frac{n+24}{8} + \frac{1}{2} \right\rfloor. \end{aligned}$$

Therefore (5) follows for all positive odd n and hence also (4). Although it is not necessary for our purpose, we can adapt the proof to show that (5) also holds for negative odd n.

Finally, to answer question (ii) we can combine (3) and (4) into a single expression. The number of bipartite theta graphs with $n \geq 5$ edges is

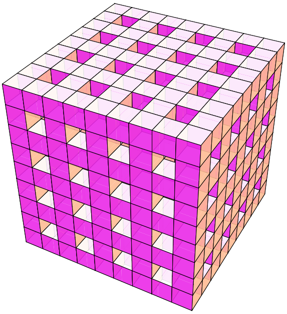
$$\left\lfloor \frac{n^2}{48} + \frac{(n \bmod 2)(n-8)}{8} + \frac{1}{2} \right\rfloor,$$

where (n mod 2) is interpreted as 0 if n is even, 1 if n is odd.

Problem 276.1 – Three dice

The television game-show host throws three dice in a manner that is invisible to you. He then reveals a die that shows the largest number. What's the probability that at least one of the other dice shows the same number?

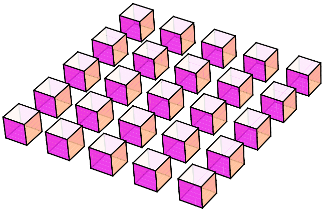
Solution 274.2 – Holey cube

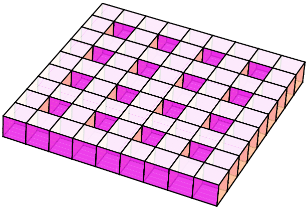


A $(2h+1) \times (2h+1) \times (2h+1)$ cube has three mutually orthogonal $h \times h$ arrays of 1×1 holes running through it. Find a formula for $c(h)$, the number of little cubes used in its construction, and $f(h)$, the number of exposed facelets. Hence or otherwise compute the limit of $f(h)/c(h)$ as h tends to infinity.

Tamsin Forbes

Let $n = 2h+1$. I shall split the cube into n slices from bottom to top. Consider two types, I and II, say.





Type-I slices (illustrated on the left for $h = 4$) occur at positions 2, 4, …, $n-1$ and each consists of an $(h+1) \times (h+1)$ array of cubes separated by holes. Clearly, there are $(h+1)^2$ cubes and $4(h+1)^2$ exposed faces.

Type-II slices (right) occur at positions 1, 3, …, n and each contains $n^2 - h^2$ cubes. Getting the number of exposed faces is a bit tricky, and we compute it as follows. There are $4n$ faces which appear on the outside of the big cube and another $4h^2$ that line the h^2 holes. But we must also count faces on the top and the bottom of each slice. Here, an exposed face will occur on one of the $n^2 - h^2$ cubes if it is not adjacent to one of the $(h+1)^2$ cubes in a type-I slice. Since a cube in a type-I slice always occurs above or below a cube in a type-II slice, there are $n^2 - h^2 - (h+1)^2$ extra faces to count on each side of the type-II slice. Putting all this together gives $4n + 4h^2 + 2(n^2 - h^2 - (h+1)^2)$ exposed faces.

There are h type-I slices and $h+1$ type-II slices. Hence

$$c(h) \;=\; h(h+1)^2 + (h+1)(n^2 - h^2) \;=\; (h+1)^2(4h+1).$$

And, remembering to add $2(h+1)^2$ for the extra faces that are exposed on the bottom and top of the structure, we have

$$\begin{aligned} f(h) \;&=\; h \cdot 4(h+1)^2 + (h+1)\left(4n + 4h^2 + 2(n^2 - h^2 - (h+1)^2)\right) \\ &\quad + 2(h+1)^2 \;=\; 6(h+1)^2(2h+1). \end{aligned}$$

Tommy Moorhouse

First we consider $c(h)$, the number of small cubes. I found the easiest way to do this was to consider the two types of 'slice' we find parallel to a given face. The first slice, the face of the large cube, contains $(2h+1)^2 - h^2$ small cubes. This kind of slice occurs $h+1$ times. The second slice contains $(h+1)^2$ small cubes, and there are h of these slices. The total number of small cubes is therefore $c(h) \;=\; (4h+1)(h+1)^2$. That is

$$c(h) \;=\; 4h^3 + 9h^2 + 6h + 1.$$

Next we think about the number of small faces ('facelets'). Each face of the large cube has $(2h+1)^2 - h^2$ facelets, and each 'tunnel' adds four faces each time it passes through each of the $(h+1)$ slices of the first kind. There are three sets of h^2 tunnels. The total number of facelets is then

$$f(h) \;=\; 6((2h+1)^2 - h^2) + 12h^2(h+1) \;=\; 12h^3 + 30h^2 + 24h + 6.$$

The ratio $f(h)/c(h)$ tends to 3. This is effectively the ratio of the total surface area to the 'mass', which for a non-holey cube is 6 in appropriate units. The 'density' of the holey cube is $c(h)/(2h+1)^3$ which tends to 1/2 the density of the individual cubes.

Tony Forbes

Counting exposed faces in holey cubes might not be entirely straightforward. So it is wise to have some idiot-proof method that can be used to check at least a finite number of individual cases. One way to compute $f(h)$ would be to build a real model, fully immerse it in paint, then disassemble and count the painted faces. I adopted a less messy approach.

To create a picture of a holey cube with parameter h, I draw a unit cube parallel to the axes and with its left-front-bottom vertex at (x, y, z) for x, y, $z = 0$, 1, …, $2h$ unless at least two coordinates are odd. A by-product of the process is a list of $c(h)$ coordinate triples from which I can generate a collection, F_h, of $6c(h)$ face-centre coordinate triples, six for each cube. Let d_h denote the number of distinct elements of F_h. Then $f(h) = 2d_h - 6c(h)$. The table shows the values obtained by this method, and, moreover, they actually agree with the given formulæ.

h	0	1	2	3	4	5	6	7	8	9	10
$c(h)$	1	20	81	208	425	756	1225	1856	2673	3700	4961
$f(h)$	6	72	270	672	1350	2376	3822	5760	8262	11400	15246

Factorization using the number field sieve – II

Roger Thompson

Continued from M500 275

Appendix A Gaussian elimination

Each candidate is of the form $\prod_{i=1}^{n} p_i^{a_i}$, where the p_i constitute the n primes in the factor base, and some a_i is odd (for otherwise, elimination would not be required). For each candidate, we keep an n bit binary number built up from the parity of each a_i (0 if even, 1 if odd). For example, if the $a_i = 0, 6, 1, 2, 1$, we would keep 00101. We need at most $n+1$ distinct binary numbers to produce a combination for which the product of the associated candidates has all even powers. To see this, consider $n+1$ distinct binary numbers in isolation, then taken in pairs XORed together, then in threes, etc. The XORing corresponds to multiplying the associated candidates together, thereby adding their powers. This gives a total of

$$\binom{n+1}{1} + \binom{n+1}{2} + \cdots + \binom{n+1}{n+1} \;=\; 2^{n+1} - 1 \;>\; 2^n - 1,$$

so not all the values can be different, in which case at least two can be XORed together to give all zeroes.

If we find that any candidate has an odd a_k for a particular k, but that no other candidate has an odd a_k, we remove that candidate. If no candidate has an odd a_k for a particular k, we ignore p_k, and therefore its bit position, so halving the number of distinct values available. Example binary numbers (after removing redundant candidates and bit positions):

A 00111, B 01101, C 10001, D 00110, E 11000, F 01011.

We aim to build up a combination of binary numbers XORed together so that their rightmost 1 bit position decreases. The rightmost bit of A is in position 5, so we have

Position	Construction	Value
1		
2		
3		
4		
5	A	00111

Consider B, whose rightmost 1 is in position 5. Position 5 is occupied, so XOR B and the entry, giving AB 01010, whose rightmost 1 is in position 4. Position 4 is empty, so add it.

Position	Construction	Value
1		
2		
3		

Position	Construction	Value
4	AB	01010
5	A	00111

Consider C, whose rightmost 1 is in position 5. Position 5 is occupied, so XOR C and the entry, giving AC 10110, whose rightmost 1 is in position 4. Position 4 is occupied, so XOR AC and the entry, giving ACAB (or CB) 11100, whose rightmost 1 is in position 3. Position 3 is empty, so add it.

Position	Construction	Value
1		
2		
3	CB	11100
4	AB	01010
5	A	00111

Consider D, whose rightmost 1 is in position 4. Position 4 is occupied, so XOR D and the entry, giving ABD 01100, whose rightmost 1 is in position 3. Position 3 is occupied, so XOR ABD and the entry, giving ABDCB (or ADC) 10000, whose rightmost 1 is in position 1. Position 1 is empty, so add it.

Position	Construction	Value
1	ADC	10000
2		
3	CB	11100
4	AB	01010
5	A	00111

Consider E, whose rightmost 1 is in position 2. Position 2 is empty, so add it.

Position	Construction	Value
1	ADC	10000
2	E	11000
3	CB	11100
4	AB	01010
5	A	00111

Consider F, whose rightmost 1 is in position 5. Position 5 is occupied, so XOR F and the entry, giving AF 01100, whose rightmost 1 is in position 3. Position 3 is occupied, so XOR AF and the entry, giving AFCB 10000, whose rightmost 1 is in position 1. Position 1 is occupied, so XOR AFCB and the entry, giving AFCBADC (or FBD) 00000, so we have found a solution.

The above illustrates that even though factorization might be thought of as an all or nothing process (either you know the answer or you don't), in some sense the solution builds up bit by bit (literally) as more and more suitable candidates are found.

Appendix B Algebraic integers and $f'(X)$

An **algebraic integer** is the root of a monic polynomial with integer coefficients. Any root α of the f we are using is an algebraic integer since we required f to be monic. From standard theory, $a + b\alpha$ is an algebraic integer if a, b are integers, so that $\prod_i (a_i + b_i\alpha)$ is also an algebraic integer. In other words, all the polynomials we have been considering modulo f are algebraic integers if $X = \alpha$. By construction, all these polynomials have integer coefficients. We will refer to the ring of such polynomials as $\mathbb{Z}[X]$. However, there may be algebraic integers whose polynomials have fractional coefficients. For example, let α be a root of our example polynomial

$$f \;=\; X^3 + 2X^2 + 5X + 1, \qquad \text{i.e.} \qquad \alpha^3 + 2\alpha^2 + 5\alpha + 1 \;=\; 0.$$

If $z = \alpha^2/3 + \alpha - 1/3$, then $z^3 + 5z^2 + 8z + 3 = 0$, but $z \notin \mathbb{Z}[\alpha]$.

We now need a few definitions and results from standard theory. Let α be a root of $f(X) = 0$, and let $\{\gamma_0, \gamma_1, \ldots, \gamma_{d-1}\}$ be a set of complex numbers. Then if for any set of rationals $q_0, q_1, \ldots, q^{d-1}$,

$$\beta \;=\; \sum_{i=0}^{d-1} q_i\alpha^i \;=\; \sum_{i=0}^{d-1} r_i\gamma_i$$

for some set of rationals $r_0, r_1, \ldots, r_{d-1}$, then $\gamma_0, \gamma_1, \ldots, \gamma_{d-1}$ is said to be a **basis** for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. We define the **trace** of β:

$$T(\beta) \;=\; \sum_{j=0}^{d-1}\sum_{i=0}^{d-1} q_i\alpha_j^i,$$

where $\alpha_0, \ldots, \alpha_{d-1}$ are the roots of $f(X) = 0$. In particular, if β is an algebraic integer, then $T(\beta)$ is an integer.

Let the monic polynomial

$$f(X) \;=\; \sum_{i=0}^{d} A_i X^i \;=\; \prod_{i=0}^{d-1} (X - \alpha_i),$$

where the α_i are the roots of $f(X)$. If any α_i is a multiple root, we can see from the product that α_i must be a root of $f'(X)$, so must be a root of $\gcd(f(X), f'(X))$. Since $f(X)$ is irreducible, this must mean $f'(X) = f(X)$, which is impossible since $\deg(f'(X)) < \deg(f(X))$; so $f(X)$ cannot have repeated roots, and hence if $f(\alpha_i) = 0$, then $f'(\alpha_i) \neq 0$. Dividing the product $\prod_{i=0}^{d-1}(X-\alpha_i)$ by $(X-\alpha_j)$ for one of the roots α_j, we can write

$$\frac{f(X)}{X-\alpha_j} \;=\; \sum_{i=0}^{d-1}\beta_i^{(j)}X^i$$

for some coefficients $\beta_i^{(j)}$.

From the definition of the derivative,

$$\begin{aligned} f'(\alpha_j) &= \lim_{\delta X\to 0}\frac{f(\alpha_j+\delta X)-f(\alpha_j)}{\delta X} \;=\; \lim_{\delta X\to 0}\frac{f(\alpha_j+\delta X)}{\alpha_j+\delta X-\alpha_j} \\ &= \lim_{X\to\alpha_j}\frac{f(X)}{X-\alpha_j} \;=\; \sum_{i=0}^{d-1}\beta_i^{(j)}\alpha_j^i, \end{aligned}$$

i.e.

$$\sum_{i=0}^{d-1}\frac{\beta_i^{(j)}\alpha_j^i}{f'(\alpha_j)} \;=\; 1;$$

so if $X=\alpha_j$,

$$\sum_{i=0}^{d-1}\frac{\beta_i^{(j)}X^i}{f'(\alpha_j)}\alpha_j^k \;=\; X^k \quad\text{for}\quad 0\le k\le d-1.$$

Then we must have

$$\sum_{j=0}^{d-1}\left[\sum_{i=0}^{d-1}\frac{\beta_i^{(j)}X^i}{f'(\alpha_j)}\alpha_j^k\right] \;=\; X^k$$

if X is any of the d distinct roots $\{\alpha_0,\alpha_1,\ldots,\alpha_{d-1}\}$. Since both sides of the equation are of degree $d-1$, the above equation must be true for all X; so

$$\sum_{j=0}^{d-1}\frac{\beta_i^{(j)}}{f'(\alpha_j)}\alpha_j^k \;=\; \begin{cases}0 & \text{if } i\ne k,\\ 1 & \text{if } i=k,\end{cases}$$

i.e. $T(\beta_i\alpha^k/f'(\alpha))=1$ if $i=k$, 0 otherwise.

For any root α, $f(\alpha)=0=\sum_{i=0}^{d}A_i\alpha^i$, so

$$f(X) \;=\; \sum_{i=0}^{d}A_i(X^i-\alpha^i),$$

giving

$$\begin{aligned}\frac{f(X)}{X-\alpha} &= \sum_{i=0}^{d-1} \beta_i X^i \;=\; \sum_{i=0}^{d} \frac{A_i(X^i-\alpha^i)}{X-\alpha} \\ &= A_1 + A_2(X+\alpha) + A_3(X^2+\alpha X+\alpha^2) + \ldots,\end{aligned}$$

and hence

$$\begin{aligned}\beta_{d-1} &= A_d = 1, \\ \beta_{d-2} &= \alpha + A_{d-1}, \\ \beta_{d-3} &= \alpha^2 + \alpha A_{d-1} + A_{d-2}, \\ &\ldots, \\ \beta_0 &= \alpha^{d-1} + \alpha^{d-2}A_{d-1} + \cdots + \alpha A_2 + A_1.\end{aligned}$$

We can see that $\beta_0, \beta_1, \ldots, \beta_{d-1}$ is a basis since

$$\sum_{i=0}^{d-1} q_i \alpha^i \;=\; q_{d-1}\beta_0 + (q_{d-2} - A_{d-1}q_{d-1})\beta_1 + \ldots;$$

so

$$\frac{\beta_0}{f'(\alpha)},\ \frac{\beta_1}{f'(\alpha)},\ \ldots,\ \frac{\beta_{d-1}}{f'(\alpha)}$$

is also a basis, and each $\beta_i \in \mathbb{Z}[\alpha]$.

Now suppose γ is an algebraic integer, with

$$\gamma \;=\; \sum_{i=0}^{d-1} \frac{s_i\beta_i}{f'(\alpha)}$$

for some rationals $s_0, \ldots, s_{d-1}$. Then

$$\alpha^k\gamma \;=\; \sum_{i=0}^{d-1} \frac{s_i\beta_i\alpha^k}{f'(\alpha)};$$

so $T(\alpha^k\gamma) = s_k$ for $k = 0, 1, \ldots, d-1$. Now for any k, $\sum_{i=0}^{d-1} \alpha_i^k$ is an integer (see my article on the Perrin sequence in M500 **269**), and $T(\gamma)$ is an integer since γ is an algebraic integer, so s_k is an integer. So for any algebraic integer γ, whether or not it has integer coefficients,

$$f'(\alpha)\gamma \;=\; \sum_{i=0}^{d-1} s_i\beta_i$$

has integer coefficients.

The remainder of this section illustrates the above analysis. For our example $f'(X) = 3X^2 + 4X + 5$, and we find

$$(3X^2 + 4X + 5)(22X^2 + 45X + 74) \;=\; 279,$$

so

$$\frac{1}{f'(X)} \;=\; \frac{22X^2 + 45X + 74}{279}.$$

We therefore have

$$\begin{aligned}
\frac{\beta_2}{f'(X)} &= \frac{22X^2 + 45X + 74}{279}, \\
\frac{\beta_1}{f'(X)} &= (X+2)\frac{22X^2 + 45X + 74}{279} \;=\; \frac{45X^2 + 54X + 126}{279}, \\
\frac{\beta_0}{f'(X)} &= (X^2+2X+5)\frac{22X^2 + 45X + 74}{279} \;=\; \frac{74X^2 + 126X + 325}{279}.
\end{aligned}$$

For the algebraic integer z in the above example, $(X^2 + 3X - 1)/3$, we find $s_2 = 19$, $s_1 = 1$, $s_0 = -5$, and

$$\begin{aligned}
\frac{19\beta_2 + \beta_1 - 5\beta_0}{f'(X)} &= \frac{1}{279}\Big((19\times 22 + 45 - 5\times 74)X^2 \\
&\quad + (19\times 45 + 54 - 5\times 126)X + (19\times 74 + 126 - 5\times 325)\Big) \\
&= \frac{93X^2 + 279X - 93}{279} \;=\; \frac{X^2 + 3X - 1}{3}.
\end{aligned}$$

Also, based on the M500 **269** article, for any monic cubic polynomial $f(X) = \sum_{i=0}^{3} A_i X^i$, $P(k) = \sum_{i=0}^{2} \alpha_i^k$ can be calculated from

$$\begin{aligned}
P(-1) &= -A_1, \quad P(0) \;=\; 3, \quad P(1) \;=\; -A_2, \\
P(n+3) &= -A_2P(n+2) - A_1P(n+1) - A_0P(n)
\end{aligned}$$

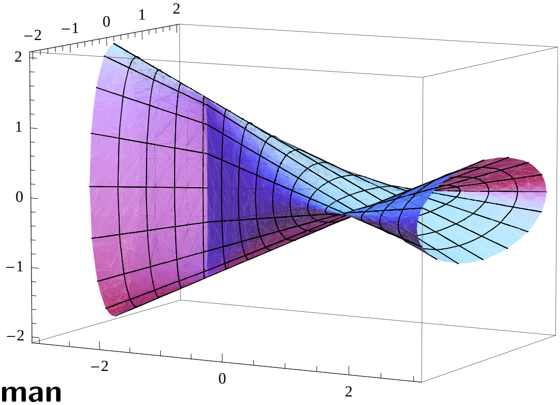
(analogous recurrence relations can easily be constructed for polynomials of other degrees). For our polynomial $X^3 + 2X^2 + 5X + 1$, this gives $P(0) = 3$, $P(1) = -2$, $P(2) = -6$; so

$$T\left(\frac{X^2 + 3X - 1}{3}\right) \;=\; P(2)\times\frac{1}{3} + P(1)\times 1 + P(0)\times\frac{-1}{3} \;=\; -5,$$

an integer.

Solution 234.1 – Two ellipses

> Let a, b and c be positive numbers with $b \neq a$. Let E_1 be an ellipse with axes $2a$ and $2b$ and situated in the plane $x = -c$ with its centre at $(-c, 0, 0)$ and its $2b$-axis vertical. Let E_2 be a similar ellipse but centred at $(c, 0, 0)$ and with its $2a$-axis vertical. Now join each point of E_1 to the diametrically opposite point of E_2. The resulting surface has two singularities in the form of straight line segments. What is the volume enclosed by the surface between the two lines?



Dick Boardman

Consider two points,

$$p_1(\theta) \;=\; (-c, a\cos\theta, b\sin\theta), \qquad p_2(\theta) \;=\; (c, -b\cos\theta, -a\sin\theta),$$

so that $p_1(\theta)$ is on ellipse E_1, $p_2(\theta)$ is the diametrically opposite point on ellipse E_2, and θ is a parameter that goes from 0 to 2π. Note, by the way, that the line segments all have the same length:

$$|p_1(\theta)p_2(\theta)| \;=\; \sqrt{(p_1(\theta) - p_2(\theta)) \cdot (p_1(\theta) - p_2(\theta))} \;=\; \sqrt{(a+b)^2 + 4c^2}.$$

Now any point on the line joining $p_1(\theta)$ and $p_2(\theta)$ is given by $kp_1(\theta) + (1 - k)p_2(\theta)$. This gives a parametric form of the surface:

$$P(k,t) \;=\; kp_1(\theta) + (1-k)p_2(\theta), \quad 0 \leq \theta \leq 2\pi, \quad 0 \leq k \leq 1.$$

Substitute $k = (c - x)/(2c)$ to get a parametric form in θ and x which will be a sequence of ellipses as x goes from $-c$ to $+c$:

$$E(x,\theta) \;=\; \left(x,\; -\frac{a(x-c) + b(x+c)}{2c}\cos\theta,\; -\frac{b(x-c) + a(x+c)}{2c}\sin\theta\right).$$

These ellipses degenerate into lines when the coefficients of $\cos\theta$ and $\sin\theta$ are zero; that is, when

$$a(x-c)+b(x+c) \;=\; 0, \quad \text{or} \quad b(x-c)+a(x+c) \;=\; 0,$$

which are solved for x to obtain

$$x \;=\; \pm\frac{(a-b)c}{a+b}.$$

The area of an ellipse is π times the product of the radii. The volume, V, enclosed by the surface between the two line segments is this area integrated from $x=-(a-b)c/(a+b)$ to $x=(a-b)c/(a+b)$. Thus

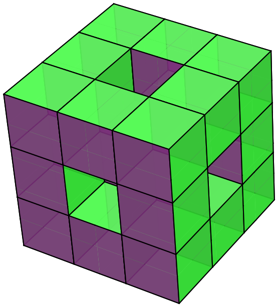
$$\begin{aligned} V &= \pi\int_{-(a-b)c/(a+b)}^{(a-b)c/(a+b)} \frac{a(x-c)+b(x+c)}{2c}\cdot\frac{b(x-c)+a(x+c)}{2c}\,dx \\ &= -\frac{(a-b)^3c\,\pi}{3(a+b)} \end{aligned}$$

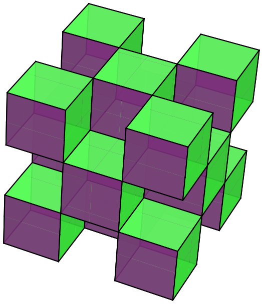
and the sign can be ignored as we are interested only in the absolute value of V.

Problem 276.2 – Cubes

An $n\times n\times n$ cube is assembled from n^3 $1\times 1\times 1$ cubes. The number of exposed faces of the little cubes is clearly $6n^2$. What is the maximum number of exposed faces that can be achieved by removing cubes from the outside of the structure?

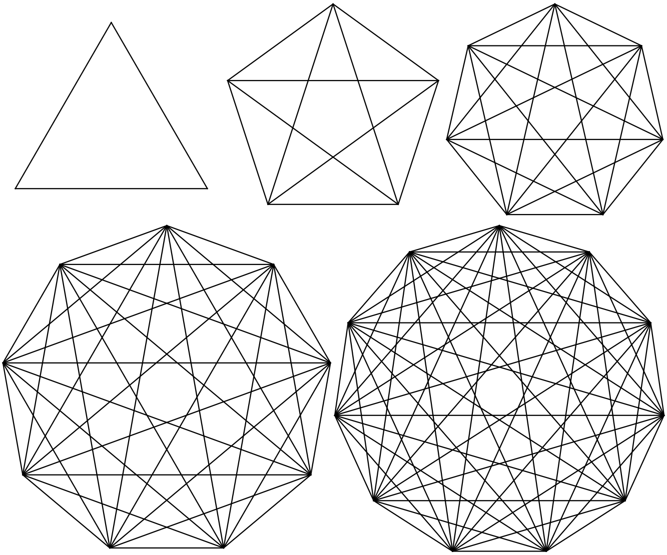
The $n=1$ case is trivial, $n=2$ is almost as easy and we did $n=3$ at the Winter Weekend. Show that either of the two arrangements shown below achieves the maximum, or find a better one. Thanks to Rob and Judith Rolfe for suggesting the problem.





Problem 276.3 – Counting triangles

How many triangles are there in each of the diagrams?



The constructions are based on regular n-gons, $n = 3$, 5, 7, 9 and 11. We did the second ($n = 5$) at the M500 Winter Weekend, where we discovered that by simple counting it is extremely easy to miss things. Is it possible to get a general formula that works for any odd n? Thanks to Rob and Judith Rolfe for suggesting the problem. The answer for the first diagram is 1.

By restricting n to odd values I (TF) hope to avoid those tiresome situations where three diagonals intersect at a single point inside the polygon. So another task for you is to prove that these triple intersections do not happen unless n is even and greater than 4.

Problem 276.4 – Symmetric binary matrix

Tony Forbes

Let $\mathbf{B}$ be a symmetric $\{0, 1\}$ matrix with diagonal elements $\mathbf{d}$. Show that $\mathbf{Bx} \equiv \mathbf{d} \pmod 2$ is solvable for $\mathbf{x}$, or find a counter-example. For instance,

$$\mathbf{B} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{d} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \pmod 2.$$

The Joy of SET

The Many Mathematical Dimensions of a Seemingly Simple Card Game

Liz McMahon, Gary Gordon, Hannah Gordon and Rebecca Gordon

Princeton University Press, 2017, ISBN 9780691166148

Tony Forbes writes: In case it is new to you, I had better state that the seemingly simple card game is SET, very popular in the Unites States and elsewhere. It has been around for about 25 years and you can find out all you need to know from http://www.setgame.com/, or look it up in *Wikipedia*. Here we restrict ourselves to a brief, simplified description.

The general idea is that in a competitive environment players attempt to identify lines in the 4-dimensional affine geometry of order 3, AG(4,3), also known to design theorists as the affine Steiner triple system of order 81. The points are represented by 81 cards with various colourful, eye-catching designs on them. You can obtain SET from shops or online, packaged in a nice plastic box like a double-pack of standard playing cards.

Play begins with the dealer dealing 12 points (cards) from the deck face-up on to the table. Thereafter, players compete with each other to find lines, which (within the context of the game) are also called *SET*s.[1] It's a free-for-all, with no orderly taking of turns. If you think you have identified a line, you say "Set!" before anyone else does so. You are then obliged—under penalty if you fail—to remove a line from the table, which if necessary is replenished with new cards to bring the number back to 12. Play continues until the deck is depleted; the winner is the person with the most lines. Occasionally a situation arises when, after staring at the table for a long time (one hour, say), all players agree that there are no *SET*s for the taking. Then the dealer would, if possible, deal three more cards.

The following shows a typical state of the game, where (for my convenience and to avoid copyright infringement) I have chosen to illustrate the twelve cards using quadruples of small integers.

(3,1,1,3)	(2,3,1,1)	(1,3,1,2)	(2,2,1,1)	(3,1,1,2)	(3,2,1,3)
(2,2,1,2)	(3,3,1,3)	(3,2,1,2)	(2,1,1,1)	(2,2,3,2)	(1,3,2,1)

The array contains seven *SET*s, (1,3,4), (1,6,8), (1,11,12), (2,3,8), (2,4,10), (3,5,7) and (3,6,10), numbering the cards 1–12 from top-left to bottom-right. As an interesting exercise, can you guess the definition of a *SET*[2] from the information I have given and before you turn over the page?

[1] Since I can't make up my mind I shall use the words {point, card} and {line, *SET*} interchangeably.

[2] This is of course fundamental to the mechanics of the game.

The book is a family venture. Liz is married to Gary and the other two authors are their daughters, both world-class experts at the game. With a modicum of detective work I think one can intelligently guess who wrote which parts. Anyway, I am sure it will appeal to readers of M500. There are two distinct sections. Chapters 1–5 are aimed at SET enthusiasts (or would-be enthusiasts) and apart from describing the SET game the purpose is to bring your mathematical skills up to a level sufficient to appreciate the wonderful world of finite geometries, which is much of the subject matter of Chapters 6–10.

Chapter 1 introduces the game, and explains how it works, how to play, how to win and how to cheat, or at least how to distract your opponents into playing poorly. Chapters 2–5 are best described as very elementary introductions to important mathematics: combinatorics (i.e. the counting of things), probability, number theory (modular arithmetic) and geometry. The pace is leisurely. The text is delightful and a joy (!) to read even if you believe yourself to be an expert on the relevant subject matter. Somewhere you will find out why you never need to have more than 21 cards on the table. And somewhere else explains how you can make the SET end-game more exciting if you deal the last card face down.

Chapters 6–10 are at a different level. Here the mathematics is more serious. Chapter 6 builds on Chapter 2, and many combinatorial problems, some of which are rather tricky, have to be resolved. We know there are 81 cards, but how many possible *SET*s[3] are there? Similarly, Chapter $i + 4$ extends the ideas introduced in Chapter i, $i = 3, 4, 5$. Chapter 9, Affine Geometry Plus, is especially interesting to me. In it I was pleasantly surprised to see some familiar objects that have appeared as cover pictures of past issues of M500. There is a photograph of a hand-made ball-and-string model of the projective geometry PG(3,2), reminding me of the projective Steiner triple system of order 15 illustrated on the cover of M500 **199**. And in the same chapter you can find a discussion of the 39 planes of AG(3,3) (front cover of M500 **219**) as well as the decomposition of the card deck into *SET*-free sets of sizes 20, 20, 20, 20 and 1. My recognition of this last item as the front-cover picture of M500 **217** was the proof I needed that *The Joy of SET* was a must-buy for me.[4]

The last chapter of the book addresses SET-related probability questions that refuse to yield to exact analysis, and so we must use computer simulations. I give just one example. How often will a SET game finish with no cards left on the table—the criterion for success if you play solitaire? Personally, I have yet to witness this happening whilst playing manually with

[3] A *SET* occurs if and only if three cards sum to (0,0,0,0) modulo 3.

[4] In addition to my complimentary copy, which became an Xmas gift for Tamsin.

a thoroughly shuffled pack. However, the book states that in a typical run of 100,000,000 solitaire games about 1.22% ended all clear. The same run produced approximately 44.5% endings with 9 *SET*-free cards, 46.8% with 6 cards and (not surprisingly!) exactly none with 3 cards. Also I have to admire the authors' computer skills. I failed miserably in my initial attempt to write a high-level program that takes less than a nanoweek to randomize the deck and play a solitaire SET game.

Obviously a book like this is not going to be just for entertainment. You are expected to do a little work. There are problems to solve (with solutions at the back) as well as many interesting mathematical and computer projects for you to explore. All in all, this is an excellent addition to the popular mathematics literature. Hopefully it will keep me off the streets and away from licensed premises for some time to come. Finally, I suppose it is appropriate to advise you, especially if ordering over the telephone, please beware of confusing this book with another of nearly the same title.

Problem 276.5 – Put that light out!

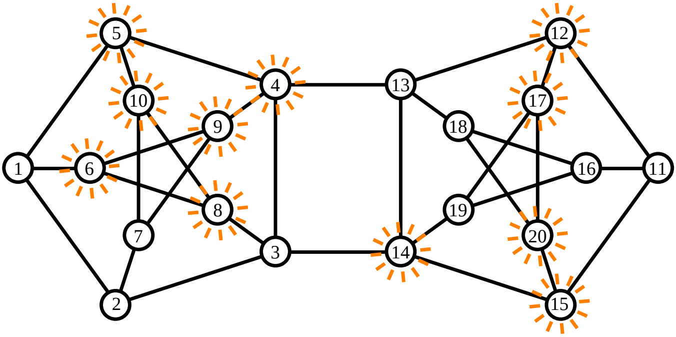
Consider an illumination facility based on a simple graph G. With each vertex v of G we associate a lamp and a push-button switch. When the switch at v is operated the lamps at v and all the neighbours of v change their states, on to off, off to on. Initially all of the lamps are lit. The objective is to switch them all off. The picture shows a typical graph with 20 vertices after switches 1, 4, 9 and 16 have been operated.

(i) Switch off the remaining lamps in the picture.

(ii) Show that the order of switching is irrelevant.

(iii) For any graph, prove that it is possible to switch all the lamps off.

Thanks to Carrie Rutherford for introducing me (TF) to the problem and for pointing out that it is a variation of the 'Lights Out' game, where G is the 5×5 grid initialized with a random selection of lights on.



Solution 184.9 – States

> What is the probability of winning a game of *Hangman* where the words are restricted to the names of USA states? Assume only one life. Assume also that you and your opponent always play sensibly.
>
> The game involves two players. At the start you choose a USA state, S, say, and you tell your opponent how many letters there are in each word of S (in the correct order if more than one). This is conveniently done by drawing an appropriate sequence of dashes. Then the following procedure is repeated until the game ends.
>
> If S is identifiable, the game ends and you lose. If not, your opponent chooses a letter, α, say. If α does not occur in S, the game ends and you win. Otherwise you reveal the position(s) of α in S.

Tony Forbes

The problem has been bothering me on and off for quite a lot of years (the reader might like to estimate how many). I have shown it to a number of mathematicians, including some who are expert game theorists, but so far without a single response. Moreover, I cannot make up my mind whether the 'experts' regard the problem as too trivial to justify their efforts, or whether it really is difficult to resolve.

The game was invented by Zoe Knight when she was about seven years old. She and I regularly and often played the usual version of Hangman (any English word and 10 lives) until one day when I noticed that all her words happened to be USA states. As you can imagine, the availability of this intelligence makes the game rather easy for the word guesser. So she suggested reducing the number of lives from 10 to 1.

To see how it works, if I, rather foolishly, were to offer '_ _ _ _ _', you would have no difficulty defeating me, assuming you are aware of the 5-letter states, IDAHO, MAINE and TEXAS. However, I can increase my chances of winning from 0 to 1/3 by choosing at random from {IOWA, OHIO, UTAH}. Then your optimal strategy, I suspect, would be to choose a letter at random from {I, A, H}. But what if I offer '_ _ _ _ _ _ _ _ _ _ _', representing a random choice from {NORTH DAKOTA, SOUTH DAKOTA}? You would start with A, which incidentally identifies or eliminates RHODE ISLAND, followed by O, T, H, D, K. But eventually you are forced to make a decision: N or S. My probability of winning is now exactly 1/2.

I have to say that I do not have a solution to the original version of the problem; i.e. I do not know of a provably best strategy for the word-setter. But in M500 **187**, I asked for a solution to the following simplification.

> Either (i) find a strategy that enables the word setter to win with probability greater than 1/2;
>
> or (ii) prove that no such strategy exists.

In other words, can I do better than choosing from {NORTH DAKOTA, SOUTH DAKOTA} with probability 1/2?

I wonder if the following idea can be made to work. There are quite a lot of 8-letter states but I am only interested in six of them, DELAWARE, ILLINOIS, KENTUCKY, MISSOURI, OKLAHOMA, VIRGINIA, and my strategy is to choose them at random with probabilities

$$d = \frac{1}{6}, \quad i = \frac{3}{20}, \quad k = \frac{1}{5}, \quad m = \frac{1}{6}, \quad o = \frac{1}{6}, \quad v = \frac{3}{20} \tag{1}$$

respectively. Assuming you are aware of these values, your choice of letter must be from Γ = {A, I, L, N, O, R} because each letter of Γ is common to three states and any other letter gives you no better than 11/30 chance of winning. With K, for example, you win only with KENTUCKY or OKLAHOMA.

Now observe that: in (1) the six fractions sum to 1, $k > 1/6$ and $k + i + v = 1/2$; N belongs to KENTUCKY whereas A, I, L, O, R do not; N also belongs to ILLINOIS and VIRGINIA; and apart from KENTUCKY each state contains precisely three letters from $\Gamma \setminus$ {N}.

Suppose you choose a letter from Γ with uniform probability, 1/6. Then you will win with probability $29/60 < 1/2$ and my strategy will have achieved its aim.

However, you notice that KENTUCKY appears significantly more often than the others. Moreover, N is the only letter of Γ in KENTUCKY. So you choose N with probability ν and the others with probability $(1 - \nu)/5$ each. We must insist that $\nu < 1$ for otherwise I will alter my strategy by omitting KENTUCKY, ILLINOIS and VIRGINIA. With this adjustment we compute the probability of you winning:

$$\nu(k + i + v) + \frac{1-\nu}{5}(3d + 3i + 3m + 3o + 3v) \;=\; \frac{24+\nu}{50} \;<\; \frac{1}{2},$$

and, again, my goal is achieved.

Solution 274.1 – Two dice

> I offer you the chance to play the following game, which is repeated until one of us becomes bankrupt.
>
> I throw two dice.
> If no 6 appears, nothing happens.
> If precisely one 6 appears, you pay me £1.
> If double-6 appears, I pay you £9.
>
> Excellent odds, you agree. Since we have eliminated the no-sixes case, the probability of getting the second 6 surely can't be less than 1/6. Well?

Dick Boardman

Probability of no sixes: $p_0 = (5/6)^2 = 25/36$; probability of exactly one six: $p_1 = 5/6 \times 1/6 \times 2 = 10/36$; probability of two sixes: $p_2 = 1/36$. This covers all cases; $p_0 + p_1 + p_2 = 1$. We play n blocks of 36 games. If the dice are random and n is large we would expect each pair to appear n times. Hence Tony will receive $10n$ units but lose $9n$. Hence the game is biased towards Tony, who will probably win in the long run.

Mike Lewis

There are 36 possible throws of two dice which are distributed as follows:

0 sixes thrown: 25, 1 six thrown: 10, 2 sixes thrown: 1.

In 36 throws in which all possible combinations occur then the following total payouts occur:

player: 10, banker: 9.

To answer the question posed, discount the 0 sixes case and the probabilities of money changing hands become

1 six thrown: 10/11, 2 sixes thrown: 1/11.

Clearly a probability of 1/11 is less than 1/6 but it is of no consequence since the payout is loaded in favour of the bank or, to be technical, the vigorish is 9.1 per cent.

Problem 276.6 – Alphabetic sum

Compute

$$\sum_{n=1}^{24} \sum_{i=1}^{n} \left((X-A)^{1-i}(X-B)^{2-i} \dots (X-Z)^{26-i}\right)^{24-n}.$$

Problem 276.7 – Three primes

If p and $p^2 + 8$ are both prime, prove that $p^3 + 4$ is also prime.

This seems to have caused a certain amount of trouble at the 2017 M500 Winter Weekend. Now I (TF) believe that I can write out a simple proof of the assertion. Unfortunately I have difficulty convincing people that my proof is correct. So I ask you to get writing. We would like to see a truly watertight proof that anybody, including non-mathematicians, can understand. Thanks to Rob and Judith Rolfe for suggesting the problem.

Problem 276.8 – Obdurate integral

Richard Gould

During the summer holiday in the middle of my sixth-form years I was given around a hundred integration problems to complete. I managed to finish most of them and, apart from one, the rest succumbed during my remaining school days. I went off to university and forgot all about the final obdurate one until I was going through my old school papers on a visit home many years later. I made further dilatory attempts on this problem over the course of many years (I wasn't a practising mathematician of any sort) but it was not until about ten years ago, spurred on by my son, that I made a really concentrated effort and finished it. My solution required a number of techniques and covered two sides of A4 paper in my fairly small handwriting. Someone reading this will certainly solve it more quickly, but I also wonder if there is a simpler solution than mine. Here it is:

$$\int \frac{\sqrt{a^2 + b^2 \cos^2 x}}{\cos x}\, dx.$$

Problem 276.9 – Sets

Tony Forbes

For $n = 1, 2, \ldots$, define the set $S(n)$ by

$$\begin{aligned} S(1) &= \{1\}, \\ S(n+1) &= \{2x + 1 : x \in S(n)\} \cup \{3x + 1 : x \in S(n)\}. \end{aligned}$$

Either show that $S(n)$ always has 2^{n-1} elements, or find a counter-example.

Contents — M500 276 – June 2017

04.01

Front cover The Hoffman–Singleton graph. Vertices on the upper pentagons are joined to vertices on the lower pentagons in a systematic manner the details of which are left for the interested reader to work out for himself or herself. The graph is 7-regular with 50 vertices and 175 edges. It has diameter 2 (two non-adjacent vertices have a common neighbour) and girth 5 (hence no triangles and no squares).