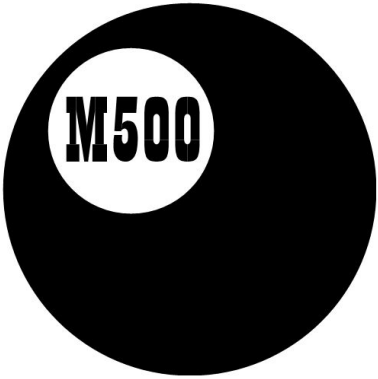
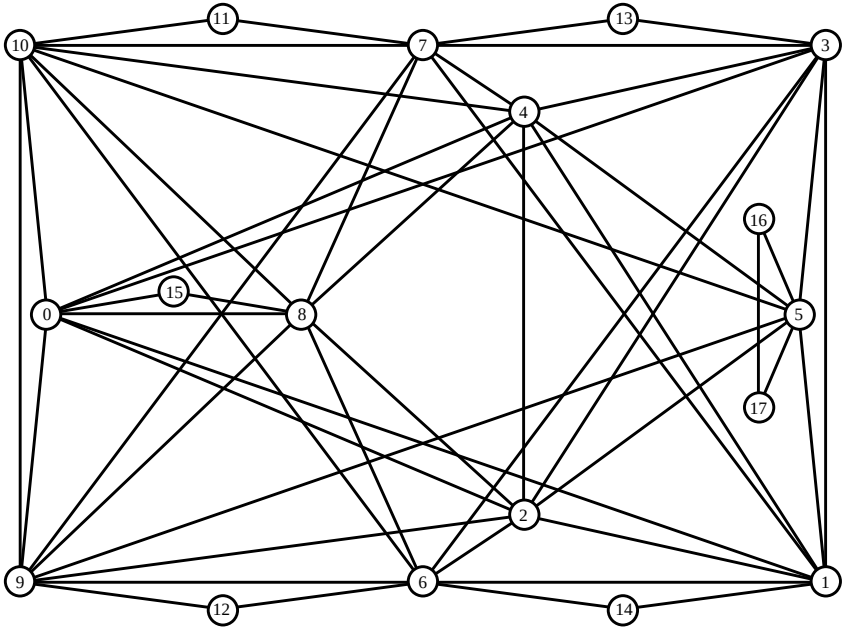
*

ISSN 1350-8539



M500 283



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 Winter Weekend 2019

The **thirty-eighth M500 Society Winter Weekend** will be held at

Florence Boot Hall, **Nottingham University**

Friday 4th – Sunday 6th January 2019.

Details, pricing and a booking form will be available nearer the time. Please refer to the M500 web site.

`m500.org.uk/winter-weekend/`

Markov chains and coupon collecting

Jon Selig

Several decades ago, while studying 'A' level mathematics, I came across a problem that I couldn't solve. I now know that the problem is usually called the 'Coupon Collector's Problem', although the version I saw concerned the collection of toys from cereal packets. The problem asked for the average number of cereal boxes you need to open to collect examples of all the toys. The question also stated that there are ten different toys distributed randomly in the cereal boxes.

I know there are fairly simple ways to solve this problem, see for example the Wikipedia page on the Coupon Collector's Problem [3]. But to be honest, I don't follow these arguments too well. So fairly recently I found a solution which uses a Markov chain to find a generating function for the distribution of waiting times.

We begin by constructing a Markov chain to model the process of collecting the coupons or opening the cereal boxes. A Markov chain is a directed graph where the nodes are states of the system, in this case we use the state to record the number of coupons/toys we have found, see Figure 1. So we begin in state 0, with no coupons. The arcs of the graph represent transitions and are labelled with the probability that that transition is taken. For example, if we are in state 0 and open a cereal box then it is certain that we will get a toy we don't already have. In state 1, if we open a box then we may or may not get a new toy. If there are k toys to collect in total then the probability that we get the same toy we already have is $1/k$ and hence the probability of getting a new toy and moving to state 2 will be $(k-1)/k$. Notice that state k is an absorbing state. Once we have found all k toys opening more boxes will not get us anything we don't already have.

The transition matrix of the Markov chain is essentially the adjacency matrix of the graph but where the non-zero entries are the probability of moving along the particular arc. That is, the rows and columns of the matrix are labelled by the states and the entry in column i row j is the probability of transitioning from state i to state j:

$$M_k = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1/k & 0 & 0 & \cdots & 0 & 0 \\ 0 & (k-1)/k & 2/k & 0 & \cdots & 0 & 0 \\ 0 & 0 & (k-2)/k & 3/k & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & (k-1)/k & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1/k & 1 \end{pmatrix}.$$

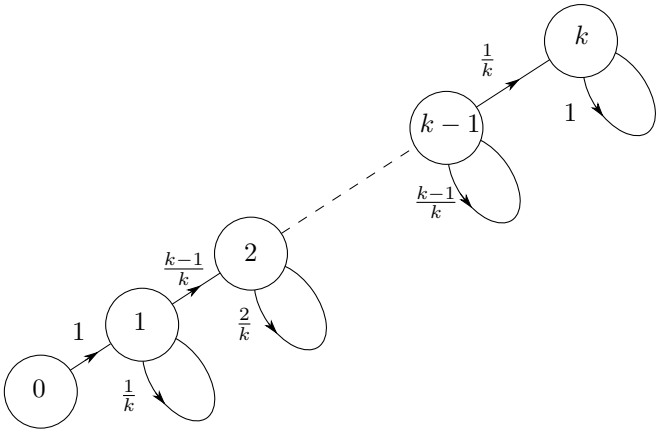


Figure 1: The Markov Chain for the Coupon Collector's Problem

To work out the probability of getting all k toys after opening n boxes, let

$$\mathbf{v}_0 \;=\; \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix};$$

this is the initial vector of occupation probabilities. After opening n boxes the probability of being in state i will be the corresponding entry in the vector

$$\mathbf{v}_n \;=\; M_k^n \mathbf{v}_0.$$

The probability of being in the final state, that is of having collected all k toys/coupons, will be given by the final entry in the vector $\mathbf{v}_n$. Let us define the vector,

$$\mathbf{e}_k \;=\; \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

to pick out the final entry, so that we can write the probability of having all k toys after opening n boxes as

$$p_k(n) \;=\; \mathbf{e}_k^T M_k^n \mathbf{v}_0.$$

This is not very easy to compute in general, so rather than attack the problem directly, suppose we try to compute the generating function of the probability distribution,

$$P_k(x) \;=\; \sum_{i=0}^{\infty} x^i p_k(i) \;=\; \sum_{i=0}^{\infty} \mathbf{e}_k^T x^i M_k^i \mathbf{v}_0.$$

This sum is simple to evaluate, since it is simply a geometric progression with 'common ratio' the matrix xM_k. The generating function can be written

$$P_k(x) \;=\; \mathbf{e}_k^T \left(I - xM_k\right)^{-1} \mathbf{v}_0.$$

Now set

$$\mathbf{v} \;=\; \left(I - xM_k\right)^{-1} \mathbf{v}_0,$$

which can be rearranged to give

$$\mathbf{v} \;=\; xM_k\mathbf{v} + \mathbf{v}_0,$$

and write the entries of $\mathbf{v}$ as $v_0, v_1, \ldots, v_k$. The matrix-vector equation above can be separated into $k+1$ simple linear equations for the unknown v_is. The first of these equations is extremely simple, $v_0 = 1$. The second equation is

$$v_1 \;=\; xv_0 + \frac{x}{k} v_1.$$

On substituting $v_0 = 1$ this simplifies to

$$v_1 \;=\; \frac{xk}{k-x}.$$

The third equation is

$$v_2 \;=\; x\frac{k-1}{k} v_1 + x\frac{2}{k} v_2.$$

Simplifying and substituting gives

$$v_2 \;=\; \frac{x(k-1)}{(k-2x)} v_1 \;=\; \frac{x^2 k(k-1)}{(k-x)(k-2x)}.$$

The next equation is

$$v_3 \;=\; \frac{x(k-2)}{k} v_2 + \frac{3x}{k} v_3$$

and from this we get

$$v_3 \;=\; \frac{x^3k(k-1)(k-2)}{(k-x)(k-2x)(k-3x)}.$$

From this the pattern is clear and we have

$$v_k \;=\; \frac{x^k k!}{\prod_{i=1}^{k}(k-ix)}.$$

Now since v_k is the last entry in $\mathbf{v}$, this is the generating function,

$$P_k(x) \;=\; \frac{x^k k!}{\prod_{i=1}^{k}(k-ix)}.$$

A standard result on power series [4] is

$$\sum_{n=0}^{\infty} S(n,\,m)z^n \;=\; \frac{z^m}{\prod_{i=1}^{m}(1-iz)},$$

where $S(n,\,m)$ is a Stirling number of the second kind. It counts the number of ways to partition a set of n elements into m non-empty subsets. We may compare this with the result for the generating function by setting $z = x/k$. Then the generating function becomes

$$P_k(x) \;=\; k!\sum_{n=0}^{\infty} S(n,\,k)\frac{x^n}{k^n}.$$

So the probability of getting all k tokens by opening at least n boxes can be seen to be

$$p_k(n) \;=\; \frac{k!}{k^n}S(n,\,k).$$

Unfortunately this is not exactly what was required. The coefficient of x^n in this generating function gives the probability that after opening n boxes we will have all k toys, and this includes the cases were we have all k toys sometime before opening the n^{th} box. What is required is the probability that it will take exactly n boxes to be opened for all k toys to be collected. That is the probability that after n boxes we have k toys but before that we don't. This problem can be addressed by modifying the Markov chain studied above; see Figure 2. An extra state can be added beyond the state where k toys have been collected. This is the new absorbing

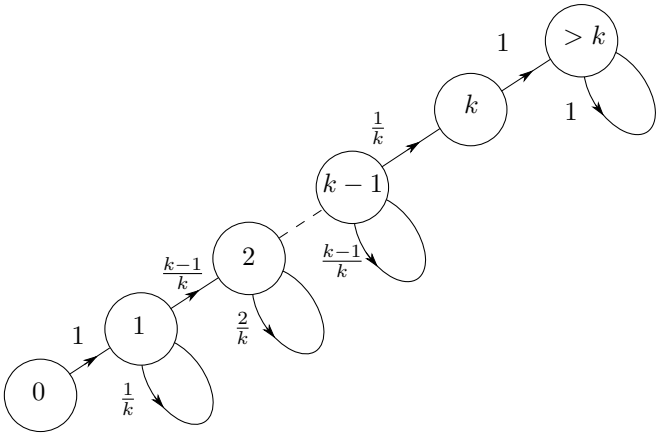


Figure 2: The Modified Markov Chain

state and the system moves to this state and stays there once all toys have been collected. The transition matrix for this chain is

$$N_k = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & \frac{1}{k} & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \frac{k-1}{k} & \frac{2}{k} & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \frac{k-2}{k} & \frac{3}{k} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \frac{k-1}{k} & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & \frac{1}{k} & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}.$$

The computation for the generating function is the same as above until we reach v_k. So we have

$$v_{k-1} = \frac{x^{k-1}k(k-1)(k-2)\cdots 2}{(k-x)(k-2x)\cdots(k-(k-1)x)},$$

but now the equation for v_k is

$$v_k \;=\; \frac{x}{k} v_{k-1}.$$

Hence, the generating function for the probability to be in state k after n trials is

$$P_k^*(x) \;=\; \frac{x^k (k-1)!}{\prod_{i=1}^{k-1}(k-ix)},$$

where the superscript $*$ is to denote the new problem. Using the same result for the expansion in terms of Stirling numbers of the second kind as above gives

$$P_k^*(x) \;=\; (k-1)! \sum_{n=0}^{\infty} S(n,\,k) \frac{x^n}{k^n} k(1-x) \;=\; k! \sum_{n=0}^{\infty} S(n,\,k)(1-x)\frac{x^n}{k^n}.$$

Assuming that $k > 0$ this can be rearranged to give

$$P_k^*(x) \;=\; k! \sum_{n=1}^{\infty} \left(\frac{S(n,\,k)}{k^n} - \frac{S(n-1,\,k)}{k^{n-1}} \right) x^n.$$

Now the recurrence relation for the Stirling numbers of the second kind is [5]

$$S(n+1,\,k) \;=\; kS(n,\,k) + S(n,\,k-1)$$

and this can be rearranged to give

$$S(n,\,k) - kS(n-1,k) \;=\; S(n-1,\,k-1)$$

and hence the generating function can be written as

$$P_k^*(x) \;=\; k! \sum_{n=1}^{\infty} S(n-1,\,k-1) \frac{x^n}{k^n}.$$

So the probability of getting all k toys in exactly n trials is

$$p_k^*(n) \;=\; \frac{(k-1)!}{k^{n-1}} S(n-1,\,k-1).$$

This result appears to be well known; it appears as an exercise in [2, p.132].

The standard method to find the expected value of a probability distribution from its generating function is to differentiate the generating function and set $x = 1$. Notice first that

$$P_k^*(1) \;=\; \frac{(k-1)!}{(k-1)(k-2)\cdots(k-(k-1))} \;=\; 1.$$

This verifies that $\sum_{n=0}^{\infty} p_k^*(n) = 1$ and hence $p_k^*(n)$ forms a probability distribution. Now differentiating the generating function gives

$$\frac{dP_k^*(x)}{dx} = \left(\frac{k}{x} + \frac{1}{k-x} + \frac{2}{k-2x} + \cdots + \frac{k-1}{k-(k-1)x}\right) P_k^*(x).$$

Substituting $x = 1$ gives

$$\frac{dP_k^*(1)}{dx} = \left(k + \frac{1}{k-1} + \frac{2}{k-2} + \cdots + \frac{k-2}{2} + k - 1\right).$$

Simplifying the fraction in this gives

$$\frac{dP_k^*(1)}{dx} = \left(k + (\frac{k}{k-1} - 1) + (\frac{k}{k-2} - 1) + \cdots + (\frac{k}{2} - 1) + (\frac{k}{1} - 1)\right).$$

Finally,

$$\frac{dP_k^*(1)}{dx} = k\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{k-1} + \frac{1}{k}\right) = kH_k,$$

where H_k is the k^{th} harmonic number.

Part of my original confusion about this problem might be explained by the fact that there are two very similar problems here. In the first we buy n cereal boxes and take our chances on getting all the toys. I guess you might do this if you really want to collect all the toys. The other problem is, to my simple mind, more realistic. We buy one box of cereal at a time until we get all the toys and then stop. When I found this connection between Markov chains and generating functions I thought it might be original but it isn't.

The method also works for other classic problems in probability; for example, finding the probability of runs of successes in a sequence of Bernoulli trials, sometimes called the 'Gambler's Ruin'. There are even more powerful techniques for solving these problems using similar ideas but based on regular languages and finite state machines rather than Markov chains; see [1], for example.

I almost forgot to answer the question! If $k = 10$, then the average number of boxes you would expect to have open to get all 10 would be

$$10\left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10}\right) = \frac{7381}{252} \approx 29.29.$$

References

[1] Flajolet, P., Gardy, D. and Thimonier, L., Birthday paradox, coupon collectors, caching algorithms and self-organizing search, *Discrete Applied Mathematics* **39** (1992), 207–229.

[2] Wilf, H. S., *Generatingfunctionology* (2nd ed.), Academic Press, 1994, ISBN 0-12-751956-4, Zbl 0831.05001.

[3] Wikipedia, Coupon collector's problem, *Wikipedia, the free encyclopedia* [Online; accessed 26 March 2018].

[4] Wikipedia, Generating Function, *Wikipedia, the free encyclopedia* [Online; accessed 26 March 2018].

[5] Wikipedia, Stirling numbers of the second kind, *Wikipedia, the free encyclopedia* [Online; accessed 26 March 2018].

Inversion as a change of coordinates

Tommy Moorhouse

Complex coordinates on the 2-sphere Consider a unit sphere S^2 centred on the origin in $\mathbb{R}^3$. The (x, y)-plane bisects the sphere, and we will think of this plane as the complex plane with coordinate w.

Projecting from the north pole A point P with coordinates (x_P, y_P, z_P) in $\mathbb{R}^3$ on S^2 can be given a complex coordinate by projecting from the north pole N (in $\mathbb{R}^3$ N has coordinates $(0, 0, 1)$). To do this extend the line NP until it intersects the (x, y)-plane at w. Calculate w in terms of (x_P, y_P, z_P).

Projecting from the south pole We can also assign a coordinate $\tilde{w}$ to P by projecting from the south pole S (coordinates $(0, 0, -1)$). Calculate $\tilde{w}$ in terms of (x_P, y_P, z_P).

Inversion Show that w and $\tilde{w}$ are related by inversion in the circle formed by the intersection of S^2 with the (x, y)-plane. Specifically, show that

$$\tilde{w} \;=\; \frac{w}{|w|^2}.$$

You could also use plane geometry to show this directly, the plane being that containing N, S and P.

Solving cubic equations modulo a prime

Roger Thompson

1 Introduction

There is a general algorithm for solving polynomial equations of any degree modulo a prime (see Cohen (2000) Algorithm 1.6.1 for example). For polynomials of degree 4 or less, there are much more efficient algorithms. This article explores algorithms for solving cubic equations modulo a prime which are considerably faster for more than 90% of primes. The algorithms make considerable use of Jacobi symbols $\left(\frac{a}{p}\right)$, which provide a very fast way of determining whether $x^2 \equiv a \bmod p$ has any solutions. There is a brief description of Jacobi symbols in my article on Perrin's sequence in M500 **269**, which contains results which we will exploit in the next section. For a particular polynomial f, $f \equiv 0 \bmod p$ has no roots for about one third of primes, one root for about a half, and three roots for about a sixth.

2 A completely general Perrin sequence

In the Perrin's sequence article, cubic polynomials of the form $f = X^3 - rX^2 + sX - 1$ were considered. Here, we consider

$$f \;=\; X^3 + PX^2 + QX + R,$$

and show what changes are required. Using the terminology of the article, define $a_f(n)$ as the sequence corresponding to f, i.e.

$$a_f(0) \;=\; 3, \quad a_f(1) \;=\; -P, \quad a_f(2) \;=\; P^2 - 2Q,$$

$$a_f(n+3) \;=\; -Pa_f(n+2) - Qa_f(n+1) - Ra_f(n).$$

Recall that the signature of n is defined as the set

$$S(n) \;=\; \{a_f(-n-1), a_f(-n), a_f(-n+1), a_f(n-1), a_f(n), a_f(n+1)\}.$$

As in the article, we can calculate $a_f(n) \bmod p$ very rapidly by repeated doubling, i.e. calculating

$$\{a_f(-2n-2), a_f(-2n), a_f(-2n+2), a_f(2n-2), a_f(2n), a_f(2n+2)\}$$

then filling in the gaps. In the general case,

$$a_f(2n) \;=\; a_f(n)^2 - 2(-R)^n a_f(-n).$$

It is not necessary to calculate the $(-R)^n$ and $(-R)^{-n}$ from scratch (for each doubling, simply square the previous value). Gaps are filled using

$$a_f(2n-1) \;=\; (PQ-R)^{-1}[-PRa_f(2n-2)-(P^2-Q)a_f(2n)+a_f(2n+2)]$$

and

$$a_f(2n+1) \;=\; (PQ-R)^{-1}[R^2a_f(2n-2)+(PR-Q^2)a_f(2n)-Qa_f(2n+2)].$$

In the article, $S_f(p)$ has particular forms, depending on the number of roots of $f \bmod p$. This is also true in the general case. In particular, we can use the value of $a_f(p+1) \bmod p$ to determine the number of roots: namely Q if there are no roots, P^2-2Q if there are three, and one for any other value. This test eliminates around one third of primes apart from those that are factors of P^2-3Q (for then the $a_f(p+1)$ values are identical).

We can actually go further. The form of $S_f(p) \bmod p$ in the general case for polynomials with a single root r (Q primes in the article) is $\{A, Q, B, B, -P, C\}$, where $A \equiv r^{-2}-2R^{-1}r \bmod p$, $C \equiv r^2-2Rr^{-1} \bmod p$ (we don't need to consider B further here). We therefore have $AC \equiv 5-2Rr^{-3}-2R^{-1}r^3 \bmod p$. Let $K = R^{-1}r^3$. Then $2K^2+(AC-5)K+2 \equiv 0 \bmod p$. Completing the square, we therefore have

$$[K+2^{-2}(AC-5)]^2 \;\equiv\; 2^{-4}(AC-5)^2-1 \bmod p.$$

We will later show how to find square roots and cube roots modulo p. However, these may yield multiple roots, or no roots at all, as the following example illustrates.

Find solutions of

$$f \;=\; X^3+X+37X+16 \;\equiv\; 0 \bmod 379.$$

We find $S_f(379) \bmod 379 = \{58, 353, 70, 70, -1, 146\}$, so we have a single root. Moreover, $2^{-2} \equiv 95 \bmod 379$, $AC-5 = 58 \times 146 \equiv 125 \bmod 379$, so we have

$$[K+95\times 120]^2 \;\equiv\; [K+126]^2 \;\equiv\; [95\times 95\times 120^2-1] \;\equiv\; 336 \bmod 379.$$

This gives $K+126 \equiv \pm 80 \bmod 379$, and hence $r^3 \equiv 22$ or $115 \bmod 379$. Now 22 has no cube roots mod 379, and 115 has three: 107, 121 and 151. Of these, 107 satisfies $X^3+X+37X+16 \equiv 0 \bmod 379$. The next section describes another method which avoids these difficulties.

3 Another approach

Before we start, we will reduce the general $Ax^3 + Bx^2 + Cx + D \bmod p$ to a simpler form. Since p is a prime, there is an integer m such that $am \equiv 1 \bmod p$, giving $x^3 + bx^2 + cx + d \bmod p$, where $b = Bm$, etc. There is an integer n such that $3n \equiv 1 \bmod p$, so that setting $x = X - bn \equiv X - b/3$, we get $X^3 + (c - nb^2)X + (d + 2n^3b^3 - nbc) \equiv 0 \bmod p$. We relabel this as $X^3 + QX + R \equiv 0 \bmod p$. If $Q = 0$, we need to find the cube root of $-R \bmod p$ (see section 6). If $Q \neq 0$, we will derive a method for solution by first looking at this equation without the modulus.

Cardano's formula for solving cubic equations, dating from the 16th century, is derived as follows: We start from the algebraic identity

$$(t-u)^3 + 3tu(t-u) - (t^3 - u^3) \;=\; 0,$$

with $X = t - u$, $3tu = Q$, $t^3 - u^3 + R = 0$. Substituting for $u = \dfrac{Q}{3t}$, we get $t^6 + Rt^3 - \dfrac{Q^3}{27} = 0$. We can solve this as a quadratic to get

$$t^3 \;=\; \frac{-R \pm \sqrt{R^2 + \dfrac{4Q^3}{27}}}{2} \;=\; \frac{-R}{2} \pm \sqrt{\frac{R^2}{4} + \frac{Q^3}{27}},$$

and

$$u^3 \;=\; t^3 + R \;=\; \frac{R}{2} \pm \sqrt{\frac{R^2}{4} + \frac{Q^3}{27}},$$

with $X = t - u$. We now make the substitutions

$$\alpha \;=\; \frac{3t^3}{Q}, \quad \beta \;=\; -\frac{3u^3}{Q}.$$

Then

$$\frac{\alpha}{\beta} \;=\; -\frac{t^3}{u^3} \;=\; z^3,$$

say, so $z = -\dfrac{t}{u}$. We find that

$$\frac{\beta z - \alpha}{z - 1} \;=\; -\frac{-3ut}{Q}\left(\frac{u^2 - t^2}{u + t}\right) \;=\; X,$$

and that

$$\alpha^2 + \frac{3R}{Q} - \frac{Q}{3} \;=\; \frac{9}{Q^2}\left(t^6 + Rt^3 - \frac{Q^3}{27}\right) \;=\; 0.$$

In other words, α is a root of $y^2 + \frac{3R}{Q}y - \frac{Q}{3} = 0$. Similar algebra shows that β is the other root. We now consider all the above modulo a prime. We have a quadratic, but we are using both roots, and we are aiming to find z, rather than z^3. All we need now is a recurrence relation to allow us to do this. We will use Lucas sequences, which are the quadratic equivalent of Perrin sequences. We will use two such sequences U, V associated with the quadratic $x^2 + Ax + B$ which have the same recurrence relation $X_n = -AX_{n-1} - BX_{n-2}$, but with different starting conditions

$$U_0 = 0, \quad U_1 = 1 \quad \text{and} \quad V_0 = 2, \quad V_1 = -A.$$

In a similar way to Perrin sequences, it can be shown that if α, β are the roots of $x^2 + Ax + B = 0$, then $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, and $V_n = \alpha^n + \beta^n$. Similar doubling techniques can be used for fast calculation of U_n, V_n using the identities

$$U_{2n} = U_n V_n, \quad V_{2n} = V_n^2 - 2B,$$
$$2V_{n+1} = -BV_n + (A^2 - 4B), \quad 2U_{n+1} = -BU_n + V_n.$$

Theory (in Morain (1989)) states that if p is of the form $3m - 1$, then $z \equiv \left(\frac{\beta}{\alpha}\right)^{m-1} \bmod p$, and that if p is of the form $3m+1$, then $z \equiv \left(\frac{\beta}{\alpha}\right)^{m+1} \bmod p$. In the first case, we have

$$X \equiv \frac{\beta z - \alpha}{z - 1} \equiv \frac{\beta^m - \alpha^m}{\beta^{m-1} - \alpha^{m-1}} \equiv \frac{U_m}{U_{m-1}} \bmod p.$$

In the second case, we have

$$X \equiv \alpha\beta \frac{U_m}{U_{m+1}} \equiv B \frac{U_m}{U_{m+1}} \bmod p$$

since $x^2 + Ax + B = (x - \alpha)(x - \beta)$.

It is worth noting that all the above works in the modulus case, even though $y^2 + \frac{3R}{Q}y - \frac{Q}{3} \equiv 0 \bmod p$ does not necessarily have solutions. For example, $X^3 + X^2 + 37X + 16 \equiv 0 \bmod 103$ has the single root 64. If we transform the equation as described above, we get $y^2 - 5y + 45 \equiv 0 \bmod 103$, which has no solutions, and yet $\frac{U_{35}}{U_{34}} \bmod 103 = 64$ as required. In other words, $\frac{\alpha^n - \beta^n}{\alpha - \beta} \bmod p$ and $\alpha^n + \beta^n \bmod p$ exist even though $\alpha \bmod p$ and $\beta \bmod p$ do not.

4 The three root case

Using a great deal of theory, Sun (2003) gives an explicit formula for finding these roots for the case $p \equiv 1 \pmod 3$, excluding a fixed number of primes: Suppose $p \equiv 1 \pmod 3$, and

$$f \;=\; X^3 + PX^2 + QX + R \;\equiv\; 0 \bmod p$$

has three roots (section 2 shows how to check this), Let $a = (P^2 - 3Q)^3$, and $b = -2P^3 + 9PQ - 27R$. Then provided p is neither a factor of a nor $(b^2 - 4a)$ (which are fixed for a given f), the following applies: Let y be such that $y^2 \equiv b^2 - 4a \bmod p$, then $z^3 \equiv 4(b - y) \bmod p$ has three solutions $\{z_i\}$, and the three solutions of $f \equiv 0 \bmod p$ are

$$\frac{(z_i - P)^2 + 3(P^2 - 4Q)}{6z_i} \bmod p.$$

Remarkably, either root of y works equally well.

Morain (1989) uses functions derived from U, V in the previous section to find one of the roots, but the method is not applicable in all cases, and requires too much theory to pursue further here.

5 Square roots modulo a prime

We wish to solve $x^2 \equiv a \bmod p$. By definition, we can only do this if a is a quadratic residue, i.e. $\left(\frac{a}{p}\right) = 1$, which in turn means $a^{(p-1)/2} \equiv 1 \bmod p$. If p is of the form $4n - 1$, then the square roots are $\pm a^{(p+1)/4}$, since $a^{(p+1)/2} \equiv a^{(p-1)/2}a \equiv a \bmod p$. With a little more work, we can use the following for p of the form $8m + 5$. Since $a^{(p-1)/2} \equiv 1 \bmod p$, we must have $a^{(p-1)/4} \equiv \pm 1 \bmod p$. In the + case, we have roots $\pm a^{(p+3)/8} \bmod p$. Otherwise, we can use another standard result $2^{(p-1)/2} \equiv -1 \bmod p$ if p is of the form $8n + 5$ to give the roots $\pm(2a)(4a)^{(p-5)/8} \bmod p$. This only leaves the case where p is of the form $8n + 1$. This can be solved using the algorithm of Tonelli and Shanks (see Cohen (2000) Algorithm 1.5.1 for example).

6 Cube roots modulo a prime

We wish to solve $x^3 \equiv a \bmod p$. By definition, we can only do this if a is a cubic residue. If so, and we find a root r, the other roots, if any, can be found by solving $X^2 + rX + r^2 \equiv 0 \bmod p$.

From standard theory, a is a cubic residue if p is of the form $3n - 1$, or if p is of the form $3n + 1$ and $a^{(p-1)/3} \equiv 1 \bmod p$. In particular, if p is of

the form $9n + k$, the following are cube roots, easily verified by cubing the definitions:

$k = 2, 5, 8$: $a^{(2p-1)/3} \bmod p$,

$k = 4$: $a^{(2p+1)/9} \bmod p$,

$k = 7$: $a^{(p+2)/9} \bmod p$.

For primes of the form $9n + 1$, a cube root algorithm based on generalized Perrin sequences is given in Cho *et al.* (2010). In brief, the idea is: given $c \bmod p$ to find a function $f = X^3 - 3X^2 + (ct^3 + 3) - 1$ that has no roots (by checking the signature $S_f(p) \bmod p$), starting from $t = 1$, and incrementing (or using a random value). The probability of doing do for a particular t value is 1/3, so there is a 90% probability of finding such a function after 6 attempts. Having found a function, a cube root is found by evaluating $a_f((p^2 + p - 2)/9) \bmod p$.

7 References

Cho, G., Koo, N., Ha, E., Kwon, S. (2010), New Cube Root Algorithm Based on Third Order Linear Recurrence Relation in Finite Field [Online]. Available at `https://eprint.iacr.org/2013/024.pdf`.

Cohen, H. (2000), *A Course in Computational Algebraic Number Theory*, New York, Springer.

Morain, F. (1989), Résolution d'équations de petit degré modulo de grands nombres premiers, *Rapport de recherche INRIA 1085*.

Sun, Z–H., (2003), Cubic and quartic congruences modulo a prime, *Journal of Number Theory* **102**, 41–89.

Problem 283.1 – Two integer equations

Tony Forbes

Given positive integers m and n, show that the number of solutions in non-negative integers of

$$x_1 + x_2 + \cdots + x_n = m - 1 \tag{1}$$

is the same as the number of solutions in non-negative integers of

$$x_1 + x_2 + \cdots + x_m = n - 1. \tag{2}$$

Construct a 1–1 mapping between the solution sets.

For example, if $m = 1$ and $n = 1000$, each of equations (1) and (2) has just one solution, $x_1 = x_2 = \cdots = x_{1000} = 0$ and $x_1 = 999$ respectively. In this case the 1–1 mapping is trivial.

Solution 196.3 – Combinatorial index

Let b be a number base. Imagine a list of all those t-digit numbers in base b which have increasing digits when read from left to right. The list is in numerical order. Let

$$N \;=\; d_t d_{t-1} \ldots d_2 d_1$$

be one of these numbers. Then the position of N in the list is given by

$$I(N) \;=\; \binom{b}{t} \;-\; \sum_{i=1}^{t} \binom{b-1-d_i}{i}.$$

To see how it works, let $b = 7$, $t = 3$. The list consists of the 35 numbers

012, 013, 014, 015, 016, 023, 024, 025, 026, 034, 035, 036,
045, 046, 056, 123, 124, 125, 126, 134, 135, 136, 145, 146,
156, 234, 235, 236, 245, 246, 256, 345, 346, 356, 456,

and, for example, if you apply the formula to 235, you should get 27.

Find a formula for the inverse function of $I(N)$. That is, given b and t, we want a function $J(n)$ which maps n to the number at position n in the list.

Steve Moon

Let us start by continuing the example given. We want to generate $N = 235$ ($d_1 = 5$, $d_2 = 3$, $d_3 = 2$) at position 27 in the list of 3-digit numbers ($t = 3$) in base $b = 7$, constructed as described. There are $\binom{b}{t} = \binom{7}{3} = 35$ numbers in all, of which $35 - 27 = 8$ exceed 235 in the list. Now define three indices, q, m, k as follows:

$$I_q = \binom{q}{1} = q, \quad I_1 = 1, I_2 = 2, \ldots;$$

$$T_k = \binom{k+1}{2}, \quad T_1 = 1, T_2 = 3, T_3 = 6, T_4 = 10, T_5 = 15, \ldots;$$

$$P_m = \binom{m+2}{3}, \quad P_1 = 1, P_2 = 4, P_3 = 10, P_4 = 20, P_5 = 35, \ldots.$$

Thus I_q are the integers, T_k are the triangular numbers and P_m are the tetrahedral (or pyramidal) numbers. Note that in the list of numbers for the example we have the following.

(i) T_k numbers start with $b-(t-1)-k$. So $T_1 = 1$ start with 4, $T_2 = 3$ start with 3, $T_3 = 6$ start with 2, $T_4 = 10$ start with 1 and $T_5 = 15$ start with 0, accounting for all 35 numbers.

(ii) P_m numbers start with the m highest permissible values. So P_3 start with 2, 3 or 4 (5 and 6 are not permissible).

(iii) Of the T_k numbers starting with $b-(t-1)-k$, T_1 have the highest permitted value for the middle digit, T_2 have the two highest permitted values, etc. So for the T_3 numbers starting with a 2, T_1 have middle digit 5 (6 is not permitted), T_2 have middle digit 4 or 5 and T_3 have middle digit 3, 4 or 5.

(iv) $d_{t-1} \geq d_t + 1$.

Next, we find the values for the indices (here k, m, q) to enable us to calculate the digits $d_t, d_{t-1}, \ldots, d_1$ (here $t = 3$). We proceed by partitioning the number of t-digit numbers larger than the one we want (here 8) as follows.

(1) Find M, the greatest m such that $P_m \leq \binom{b}{t} - n = 8$.

(2) Find K, the greatest k such that $T_k \leq \binom{b}{t} - n - P_M = 4$.

(3) Find Q, the greatest q such that $I_q \leq \binom{b}{t} - n - P_M - T_K = 1$.

In our example,

$$M = 2, \quad P_M = 4, \quad K = 2, \quad T_K = 3, \quad Q = I_Q = 1,$$

and we have $P_M + T_K + I_Q = 8$, as wanted.

Now we turn to deriving the digits d_3, d_2, d_1. For d_3, the highest starting value is

$$b - 1 - (t-1) = b - t = 4.$$

But we have counted back past the P_2 numbers starting with the highest values 3, 4. Hence

$$d_3 = b - t - M = 7 - 3 - 2 = 2.$$

For d_2, the highest permitted middle digit value is $b - 1 - (t-2) = 5$. But by finding $T_K = T_2 = 3$ we counted back past the numbers with the top two middle digit values, 4, 5. Hence

$$d_2 = b - t + 1 - K = 7 - 3 + 1 - 2 = 3.$$

For d_1, the highest permitted middle digit value is $b-1-(t-3)=6$. But we counted back past the $I_Q = I_1 = 1$ number with last digit 6. Hence

$$d_1 \;=\; b-t+2-Q \;=\; 7-3+2-1 \;=\; 5.$$

Therefore, by partitioning the number of t-digit numbers exceeding N in this way we can derive the digit values. Here we have shown that for $b=7$, $t=3$ and $n=27$, we have $N=235$, using the indices of integers, triangular numbers and tetrahedral numbers to partition the 3-digit numbers exceeding N.

If we set $t=4$, we have a four-step process. We need 4 indices, and the first partition of the larger numbers is done using the index r defined by

$$S_r = \binom{r+3}{4}, \quad S_1 = 1,\;\; S_2 = 5,\;\; S_3 = 15,\;\; S_4 = 35,\;\; S_5 = 70,\;\; \ldots.$$

We then proceed to find the maximum values R, M, K and Q as before.

The process is easily extended to larger bases and larger values of t. For t-digit numbers, we need t indices to maximize sequentially for the partitioning.

This is effectively an algorithm. However, I'm not clear it readily lends itself to a one-line formula.

Problem 283.2 – Another determinant

This is very similar to Problem 282.5, except that the answer is very different. Compute

$$\mathrm{L}(n,\lambda) \;=\; \det \begin{bmatrix} n & n-\lambda & \ldots & n-\lambda & n-\lambda \\ n-\lambda & n & \ldots & n-\lambda & n-\lambda \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ n-\lambda & n-\lambda & \ldots & n & n-\lambda \\ n-\lambda & n-\lambda & \ldots & n-\lambda & n \end{bmatrix},$$

where n is the number of rows (or columns) in the matrix.

Problem 283.3 – Tilings

(i) Can you tile the plane with integer-sided rectangles where all the dimensions are distinct? That is, for any two rectangles, $a \times b$ and $c \times d$, the lengths a, b, c and d are distinct integers.

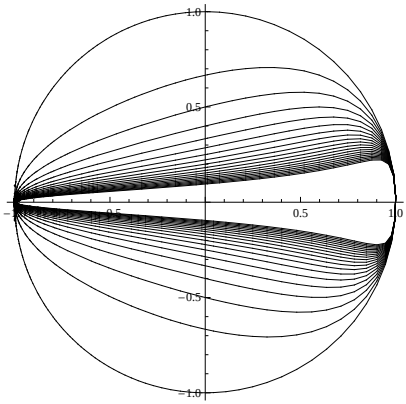
(ii) What about distinct integer-sided squares?

(iii) Equilateral triangles?

Solution 280.7 – Convex to concave

Let w be a positive number and consider the mappings $f_w(t)$ defined by

$$f_w(t) \;=\; \left(\frac{1-t^2}{1+t^2},\; \frac{2t}{1+wt^2}\right).$$

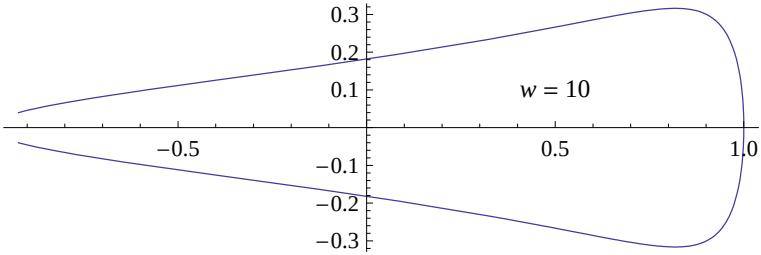


We have plotted $f_w(t)$, $-\infty < t < \infty$, for $w = 1, 2, \ldots, 20$. Recall that $f_1(t)$ gives the familiar parametrization of a circle of radius 1 centred at $(0, 0)$, and this is indeed the outermost closed curve in the picture. Thereafter the curves shrink as the parameter w increases.

Observe that the first few curves are convex and the last few are not. So there must be a special number W, where the curve is convex if $w < W$ and not if $w > W$. What is the value of W?

Dick Boardman

If a point moves around a convex closed curve, the direction of the tangent always moves in one direction. If there is a concave section, the second derivative becomes zero.



Writing

$$x(t) \;=\; \frac{1-t^2}{1+t^2}, \qquad y(t) \;=\; \frac{2t}{1+wt^2},$$

we compute the first derivative, $dy/dx = (dy/dt)/(dx/dt)$:

$$\frac{dx}{dt} \;=\; \frac{-4t}{(1+t^2)^2}, \qquad \frac{dy}{dt} \;=\; \frac{2-2t^2w}{(1+t^2w)^2}, \qquad \frac{dy}{dx} \;=\; \frac{(1+t^2)^2(t^2w-1)}{2t(t^2w)^2+1}.$$

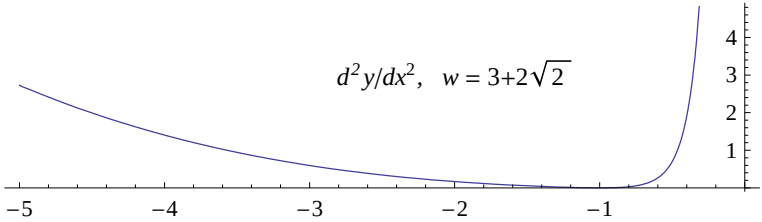
For the second derivative, we have

$$\begin{aligned}\frac{d^2y}{dx^2} &= \frac{d(dy/dx)}{dt}\Big/\frac{dx}{dt} \\ &= -\frac{(1+t^2)^3(1-3t^4(-2+w)w+t^6w^2+t^2(-3+6w))}{8(t+t^3w)^3}.\end{aligned}$$

Now let $W = 3 + 2\sqrt{2}$ and write $g(t)$ for the result of substituting W for w in d^2y/dx^2. Then

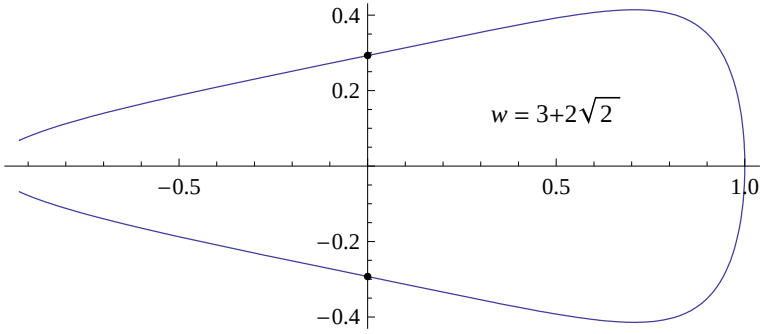
$$g(t) = \left.\frac{d^2y}{dx^2}\right|_{w=W} = -\frac{(t^2-1)^2(t^2+1)^3(1+(17+12\sqrt{2})t^2)}{8(t+(3+2\sqrt{2})t^3)^3}.$$

Clearly $g(\pm1) = 0$, and the plot below appears to show that $g(t)$ is always non-negative when $t < 0$.



To prove this we find the minimum of $g(t)$ in the usual way by computing the roots of dg/dt. However, the presence of the factor $(t^2-1)^2$ in the expression for $g(t)$ indicates that dg/dt does indeed have roots at $t = \pm1$ and hence that $g(-1) = 0$ is the minimum of $g(t)$ in the range $t < 0$.

The final plot shows the curve when $w = W$. The dots correspond to $t = \pm1$.



Problem 283.4 – Trackword

Jeremy Humphries

V	**T**	**E**
O	**A**	**I**
U	**R**	**F**

When my aged father-in-law has finished with his weekly *Radio Times*, I take it to do the puzzles (Crossword, Sudoku, Countdown numbers game, etc.). One of the puzzles is called Trackword.

They give you a 3×3 grid with letters, like that, and ask you to find as many real English words as you can, of three or more letters, by tracking from square to adjacent square, going horizontally, vertically or diagonally, and not using any square more than once per word. For instance in the grid here you could have TOUR, because that's a legal path, but not RATIO, because the I square and the O square are not adjacent, and not TAROT, because you can't use the T square twice.

The first question here is: How many legal paths are there? We don't insist on real English words, just strings of three or more letters, tracking through adjacent squares and not going anywhere more than once.

The second question here is: Can you do some generalizing?

Solution 279.8 – Arithmetic

(i) Show that

$$\frac{12 + 144 + 20 + 3\sqrt{4}}{7} + 5 \cdot 11 \;=\; 9^2 + 0. \qquad (*)$$

(ii) Translate $(*)$ into limerick form.

Chris Pile

This problem seemed to be fun
I thought that it couldn't be done.
Then—relief from depression
The left hand expression
Was found to be (just) eighty-one.

To twelve plus its square plus a score
Add three times the square root of four.
Divide this by seven,
Add five times eleven,
Which equates to nine squared (plus no more).

Problem 283.5 – Primes

Tony Forbes

Show that

$$\lim_{N\to\infty} \left(\prod_{\substack{p\le N,\ p \text{ prime} \\ p\equiv 1 \pmod 4}} \frac{p}{p-1} \right) \left(\prod_{\substack{p\le N,\ p \text{ prime} \\ p\equiv 3 \pmod 4}} \frac{p}{p+1} \right) = \frac{\pi}{4}.$$

Problem 283.6 – Pistachio nuts

They just will not go away! Here is yet another problem about pistachio nuts and the consumption thereof, the fourth, TF thinks, that we have printed in this magazine.

Ralph Hancock

A bowl contains n pistachio nuts and an equal number of empty half shells. You can't see what you are taking from the bowl, and may therefore get a nut or a half shell. A single pistachio nut supplies 10 kcal of energy, but 0.1 kcal is used in opening the shell and eating the nut. Also, 0.1 kcal is used in removing an object from the bowl, and another 0.1 kcal in replacing an object in the bowl.

You can therefore devise a bizarre and pointless ritual of removing, opening and eating nuts, and replacing some or all of the half shells or unopened nuts in the bowl, that will ensure that you gain or lose no energy by consuming all the nuts. What is the simplest ritual, i.e. involving the fewest actions, that will produce this result for any value of n?

Answers to quiz in Issue 282 (1) Douglas Adams, *Mostly Harmless*, forty-two; (2) Rudyard Kipling, *Captains Courageous*, Forty-two; (3) II Chronicles, Forty and two; (4) Thomas Hardy, *A Pair of Blue Eyes*, forty-two; (5) Oscar Wilde, *The Importance of Being Earnest*, forty-two; (6) Numbers, forty and two; (7) J. R. R. Tolkien, *The Lord of the Rings: The Two Towers*, Forty-two, forty-second; (8) Lewis Carroll, *The Hunting of the Snark*, forty-two; (9) Charles Dickens, *The Pickwick Papers*, Forty-two; (10) Arthur Conan Doyle, *The Priory School*, forty-two; (11) Douglas Adams, *The Restaurant at the End of the Universe*, Forty-two; (12) Lewis Carroll, *Phantasmagoria*, forty-two; (13) Ezra, forty and two; (14) Herman Melville, *Moby-Dick*, forty-two; (15) Charles Dickens, *A Tale of Two Cities*, forty-two; (16) *The Egyptian Book of the Dead*, two and forty; (17) George Eliot, *Middlemarch*, forty-two; (18) Jules Verne, *Around the World in 80 Days*, forty-second; (19) D. H. Lawrence, *Sons and Lovers*, 42; (20) A. A. Milne, The Morning Walk, *Now We Are Six*, forty-two; (21) John Steinbeck, *Grapes of Wrath*, forty-two; (22) Herman Melville, *Typee: A Peep at Polynesian Life*, 42; (23) II Kings, two and forty; (24) Stephen Crane, *The Red Badge of Courage*, forty-two; (25) Revelation, forty and two; (26) Leo Tolstoy, *Anna Karenina*, forty-two; (27) Lewis Carroll, *Alice's Adventures in Wonderland*, Forty-two; (28) Charles Dickens, *Oliver Twist*, forty-two; (29) *Romeo and Juliet*, two-and-forty; (30) Douglas Adams, *The Hitchhiker's Guide to the Galaxy*, Forty-two.

04.00

Front cover A 17-block partial Steiner triple system on 18 points. The seventeen triples are {0,1,2}, {0,3,4}, {1,3,5}, {2,3,6}, {1,4,7}, {2,4,8}, {2,5,9}, {4,5,10}, {6,8,10}, {7,8,9}, {0,9,10}, {11,7,10}, {12,6,9}, {13,3,7}, {14,1,6}, {15,0,8}, {16,17,5} most of which appear as thin triangles. The system is interesting because the edges that remain after removing the 17 triangles from the complete graph K_{18} on the same set of points leaves a graph with 18 vertices and 102 edges, which can be decomposed into 17 tetrahedra. It is even more interesting because I (TF) claim, on the basis of what I believe to be an exhaustive search, that the system is up to isomorphism the *only* 17-block PSTS(18) that has this property. If anyone discovers any other noteworthy properties of this thing, I really would like to know. It appears in [A. D. Forbes and T. S. Griggs, Designs for graphs with six vertices and nine edges, *The Australasian Journal of Combinatorics* **70** (2018), 52–74].