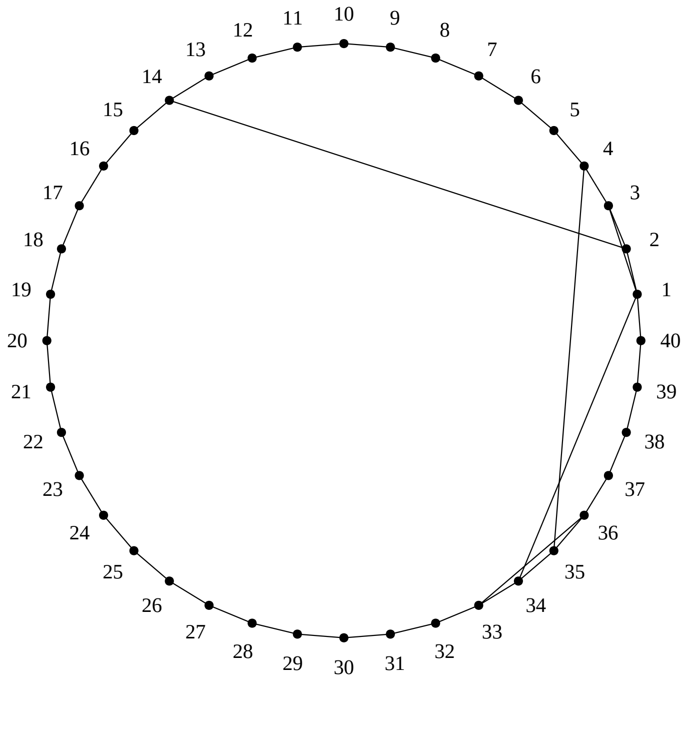
*

ISSN 1350-8539

M500 256



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 May Weekend is a residential Friday to Sunday event providing revision and examination preparation for both undergraduate and postgraduate students. For full details and a booking form see m500.org.uk/may.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details see m500.org.uk/winter.htm.

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.

Donald Preece

We are sorry to hear that Donald Preece, Emeritus Professor of Combinatorial Mathematics at the University of Kent, died on 6 January 2014 at the Western Infirmary, Edinburgh. He was a virtuoso pianist and some of you will remember his performance, dressed in his Ruritanian army outfit, as our guest lecturer at the M500 September Weekend of 2003. He was also our guest speaker in 2010.

The χ^2 distribution

Ken Greatrix

Following the success I had in compiling and using a robust version of the Standard Normal Distribution [M500 **249**, page 12] and requiring a continuous reference for another computer project, I set about making a robust version of the χ^2 distribution.

From the internet, I had found the formula for the PDF as

$$f_\nu(x) \;=\; \frac{x^{(\nu-2)/2}e^{-x/2}}{2^{\nu/2}\Gamma\big(\nu/2\big)}.$$

Also widely published on the internet is the Gamma function:

$$\Gamma(1) = 1, \qquad \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}, \qquad \Gamma(n+1) = n\Gamma(n),$$

and if n is an integer, then $\Gamma(n+1) = n!$.

As before, direct integration of the expanded formula caused overload errors and program crashes if too many terms were used in the resulting series. A consequence of using fewer terms in the expansion was that as the value of ν increased, the results 'drifted' away from the values given in published tables (as in, for example, *Elementary Statistics Tables* by Henry R. Neave). This became very noticeable even with values as low as $\nu = 10$, particularly for the higher percentages of the CDF. (Note that in the following integrations, for all values of ν, $x = 0 \Rightarrow f_\nu(0) = 0$ and also for the CDF, $F_\nu(0) = 0$. For this reason, I need not show a constant of integration). It is more convenient to separate the formula into two parts: for ν even and for ν odd.

Firstly for ν even: $\nu = 2$, substituted into the PDF gives

$$f_2(x) \;=\; \frac{x^0\; e^{-x/2}}{2^1\;\Gamma(1)}.$$

When this expression is simplified, its integration can be expressed as

$$F_2(x) \;=\; \int_0^x \frac{e^{-z/2}}{2} dz$$

(using z as an auxiliary variable). Thus

$$F_2(x) \;=\; \Big[-e^{-z/2}\Big]_0^x \;=\; 1 - e^{-x/2}.$$

Repeating this for $\nu = 4$:

$$f_4(x) \;=\; \frac{x^1\; e^{-x/2}}{2^2\;\Gamma(2)}.$$

Simplifying this and showing it as an integration gives

$$F_4(x) \;=\; \int_0^x \frac{z\; e^{-z/2}}{2^2\;\Gamma(2)} dz \;=\; 1 - e^{-x/2} - \frac{x}{2}\,\frac{e^{-x/2}}{\Gamma(2)} \;=\; F_2(x) - \frac{x}{2}\,\frac{e^{-x/2}}{\Gamma(2)}$$

and, by a similar process,

$$F_6(x) \;=\; F_4(x) - \left(\frac{x}{2}\right)^2 \frac{e^{-x/2}}{\Gamma(3)}.$$

After repeating this process a few more times, I found that I had a basis for mathematical induction. In which case, for even values of ν, I assumed that

$$F_{\nu+2}(x) \;=\; F_\nu(x) - \left(\frac{x}{2}\right)^{\nu/2} \frac{e^{-x/2}}{\Gamma\big((\nu+2)/2\big)}.$$

Making the inductive step,

$$f_{\nu+2}(x) \;=\; \frac{x^{\nu/2} e^{-x/2}}{2^{(\nu+2)/2}\Gamma\big((\nu+2)/2\big)},$$

$$F_{\nu+2}(x) \;=\; \int_0^x \frac{z^{\nu/2} e^{-z/2}}{2^{(\nu+2)/2}\Gamma\big((\nu+2)/2\big)} dz,$$

and applying integration by parts,

$$g(z) = z^{\nu/2}, \quad h'(z) = e^{-z/2}, \quad g'(z) = \frac{\nu}{2} z^{(\nu-2)/2}, \quad h(z) = -2e^{-z/2},$$

we get

$$F_{\nu+2}(x) \;=\; \left[\frac{-2z^{\nu/2} e^{-z/2}}{2^{(\nu+2)/2}\Gamma\big((\nu+2)/2\big)}\right]_0^x - \int_0^x \frac{\nu}{2}\, \frac{z^{(\nu-2)/2}\left(-2e^{-z/2}\right)}{2^{(\nu+2)/2}\Gamma\big((\nu+2)/2\big)} dz.$$

Simplifying this expression we get

$$F_{\nu+2}(x) \;=\; \frac{-x^{\nu/2} e^{-x/2}}{2^{\nu/2}\Gamma\big((\nu+2)/2\big)} + \int_0^x \frac{z^{(\nu-2)/2}\; e^{-z/2}}{2^{\nu/2}\;\Gamma\big(\nu/2\big)} dz$$

$$= F_\nu(x) - \left(\frac{x}{2}\right)^{\nu/2} \frac{e^{-x/2}}{\Gamma\big((\nu+2)/2\big)},$$

which is as I had assumed.

The function when ν is odd is not as straightforward. When $\nu = 1$,

$$f_1(x) = \frac{x^{-1/2}e^{-x/2}}{2^{1/2}\Gamma\big(1/2\big)}.$$

Integrate for the CDF:

$$F_1(x) = \int_0^x \frac{z^{-1/2}e^{-z/2}}{2^{1/2}\Gamma\big(1/2\big)} dz.$$

I know of no straightforward technique to complete this integration so I apply the technique that I demonstrated in my previous article. In brief, this is: expand the exponential term into its series form, multiply by the term in x and then integrate each term in the resulting series.

1. Extract any common factor, then show the resulting series as a sum of two other series—an exponential series and a remainder series.

2. Repeat from 1 on each successive remainder series until sufficient terms have been generated to give the desired accuracy. The result of this process is a formula that can be easily put into recursive form ready for computer programming.

Expand the x-terms of the above formula (I will ignore the constant terms for the time being):

$$\begin{aligned} x^{-1/2}e^{-x/2} &= x^{-1/2}\left(1 - \frac{x}{2} + \cdots + (-1)^k \left(\frac{x}{2}\right)^k \frac{1}{k!} + \ldots\right) \\ &= x^{-1/2} - \frac{x^{1/2}}{2} + \frac{x^{3/2}}{2^2}\frac{1}{2!} - \frac{x^{5/2}}{2^3}\frac{1}{3!} + \cdots + (-1)^k \frac{x^{(2k-1)/2}}{2^k}\frac{1}{k!} + \ldots. \end{aligned}$$

Integrate with respect to x:

$$2x^{1/2} - \frac{2}{3}x^{3/2}\frac{1}{2} + \cdots + \frac{2(-1)^k}{2k+1}x^{(2k+1)/2}\frac{1}{2^k}\frac{1}{k!} + \ldots.$$

(In the following, for convenience, ease of handling and clarity I only consider the relevant section of the series under consideration.) Extract the common factor, $2x^{1/2}$, and then rearrange the result as a sum of two series:

$$1 - \frac{x}{2} + \left(\frac{x}{2}\right)^2 \frac{1}{2!} - \left(\frac{x}{2}\right)^3 \frac{1}{3!} + \cdots + (-1)^k \left(\frac{x}{2}\right)^k \frac{1}{k!} + \ldots$$

and the remainder series,

$$\frac{2}{3}\cdot\frac{x}{2}-\frac{4}{5}\left(\frac{x}{2}\right)^2\frac{1}{2!}+\frac{6}{7}\left(\frac{x}{2}\right)^3\frac{1}{3!}+\cdots+(-1)^k\,\frac{k+2}{k+3}\left(\frac{x}{2}\right)^{k+1}\frac{1}{(k+1)!}+\cdots.$$

The first series is $e^{-x/2}$, and after $x/3$ is extracted from the second as a common factor the process is repeated:

$$\frac{x}{3}\left(1-\frac{3}{5}\cdot\frac{x}{2}+\frac{3}{7}\left(\frac{x}{2}\right)^2\frac{1}{2!}-\frac{3}{9}\left(\frac{x}{2}\right)^3\frac{1}{3!}+\cdots+(-1)^k\,\frac{3}{2k+3}\left(\frac{x}{2}\right)^k\frac{1}{k!}+\ldots\right).$$

The series in the larger brackets can again be split into two component series, one being $e^{-x/2}$ and the other the next remainder series:

$$\frac{2}{5}\cdot\frac{x}{2}-\frac{4}{7}\left(\frac{x}{2}\right)^2\frac{1}{2!}+\frac{6}{9}\left(\frac{x}{2}\right)^3\frac{1}{3!}+\cdots+(-1)^k\,\frac{k+2}{k+3}\left(\frac{x}{2}\right)^{k+1}\frac{1}{(k+1)!}+\cdots$$

with $x/5$ as its common factor. (In the above expressions, the indexing integer, k, is nominal and does not necessarily transfer its value between those expressions.)

Then, after putting all the component parts together (and including the previously ignored constants and common factors), we arrive at

$$F_1(x) \;=\; \frac{2\sqrt{x}}{2^{1/2}\Gamma(1/2)}\left(e^{-x/2}+\frac{x}{3}\left(e^{-x/2}+\cdots+\frac{x}{2k+3}\left(e^{-x/2}+\ldots\right)\right)\right).$$

Since x is likely to remain finite $x/(2k+3)\Rightarrow 0$ as $k\Rightarrow\infty$, so with a sufficiently high value of k, the subsequent terms in this recursive formula can be ignored. The recursion is started with this high value of k, which is then reduced in value until $k=0$ (for the $x/3$ term).

In testing this part of the formula in the program I called a subroutine twice, first with a high value of k (I actually used $k=20{,}000$) and then with a reducing value until a difference in the two results occurred. From this process I conclude that a k-value of approximately 350 should be sufficient for most practical purposes, this being to provide accuracy to six places of decimals. Anyone using this process should bear in mind that for more accuracy, a higher value of k may be required.

For increasing odd values of ν, the process is much the same as for the even values shown above, and with the same result:

$$F_3(x) \;=\; F_1(x)-\left(\frac{x}{2}\right)^{1/2}\frac{e^{-x/2}}{\Gamma(3/2)},$$

$$
\begin{aligned}
F_5(x) &= F_3(x) - \left(\frac{x}{2}\right)^{3/2} \frac{e^{-x/2}}{\Gamma\bigl(5/2\bigr)},\\
F_7(x) &= F_5(x) - \left(\frac{x}{2}\right)^{5/2} \frac{e^{-x/2}}{\Gamma\bigl(7/2\bigr)}.
\end{aligned}
$$

Then after applying a process of mathematical induction:

$$
F_{\nu+2}(x) = F_\nu(x) - \left(\frac{x}{2}\right)^{\nu/2} \frac{e^{-x/2}}{\Gamma\bigl((\nu+2)/2\bigr)}.
$$

There is one more hurdle remaining! There is no direct inverse calculation for a specific percentage of the CDF and so another interactive process had to be written into the program for this. It's a bit more tedium, but presents no great hardship.

At some stage while compiling this account I felt that I had been 'bitten by the bug' and decided that I should look into other similar integrations. However, I gave up on this as M500 readers would probably get bored with repeats of the same process but with different numbers. Perhaps it's a known technique, and all I've done is 're-invent the wheel'. If not then it would be interesting to discover the accepted method. Also of interest is its accuracy compared with other methods. With any repetitive process, errors can accumulate. Just because I have the same result with two sufficiently high k values which match the tables to four places of decimals doesn't mean that I have an accuracy equal to the accepted method.

Instead of repeating the technique for similar integrations, I have decided to construct a general formula for the recursive process. The main reason is that in the previous article, I claimed that *'I am certain that this expression can be proven by induction.'* Such claims should never be made by a mathematician unless a proof actually exists or can be constructed. The resulting article is complete but is still in rough draft form and will be submitted for publication in due course. I had already decided to write this general proof while compiling the above and that is why I didn't make an attempt at a proof here either.

I blink, therefore eye am.

I didn't sink, therefore I swam.

And in case you are thinking they can't possibly get any worse,

I mink, therefur I am.

Solution 253.1 – A Diophantine equation

Given that $P = 2$, $Q = 1$, and $R = 7$ is a solution to the Diophantine equation

$$P^4 + 8P^2Q^2 + Q^4 \;=\; R^2, \tag{1}$$

use this to find further solutions.

Tony Forbes

We saw in Vincent Lynch's article [M500 **254**] how points on the elliptic curve

$$\mathcal{C}: \quad y^2 \;=\; x^3 - 16x^2 + 60x$$

yield solutions of (1) via the substitutions

$$p = \frac{y}{2x}, \quad r = p^2 + 4 - \frac{30}{x}, \quad P = |Qp|, \quad R = |Q^2 r|,$$

where Q is any integer that makes P and R integers[1]. So we get these solutions obtained by successive doubling in the elliptic curve group of $\mathcal{C}$.

x	y	p	r	P	Q	R
30	120	2	7	2	1	7
$\frac{49}{4}$	$\frac{105}{8}$	$\frac{15}{28}$	$\frac{1441}{784}$	15	28	1441
$\frac{2076481}{176400}$	$\frac{812768671}{74088000}$	$\frac{564031}{1210440}$	$\frac{2444755743361}{1465164993600}$	564031	1210440	2444755743361

We wish to study this process in a little more detail and for that purpose it would be useful to have the group addition formula. However, it is not a great deal of effort to develop the formula for the general curve

$$y^2 \;=\; x^3 + ax^2 + bx + c, \tag{2}$$

and so this is what we will do. Denote the group operation by $\oplus$ and its identity by $O = (\infty, \infty)$, the 'point at infinity'. Given points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the curve, we shall obtain an explicit formula for $P_3 = (x_3, y_3) = P_1 \oplus P_2$, which is defined as the point $(x_3, -y_3)$ (note the minus sign) where the line joining P_1 and P_2 again meets the curve.

[1] The elliptic curve in M500 **254** was actually $Y^2 = 30X^3 - 16X^2 + 2X$ but the coefficient 30 of X^3 makes life slightly awkward; so I have transformed it away by substituting $X = x/30$, $Y = y/30$. The only immediate effect is that r has $-30/x$ instead of $-1/X$.

The line is

$$y = \lambda x + \mu, \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \mu = y_1 - \lambda x_1,$$

unless $P_1 = P_2$ when we use instead the slope of the tangent at P_1 for λ,

$$\lambda \;=\; \frac{dy}{dx}(x_1) \;=\; \frac{3x_1^2 + 2ax_1 + b}{2y_1}.$$

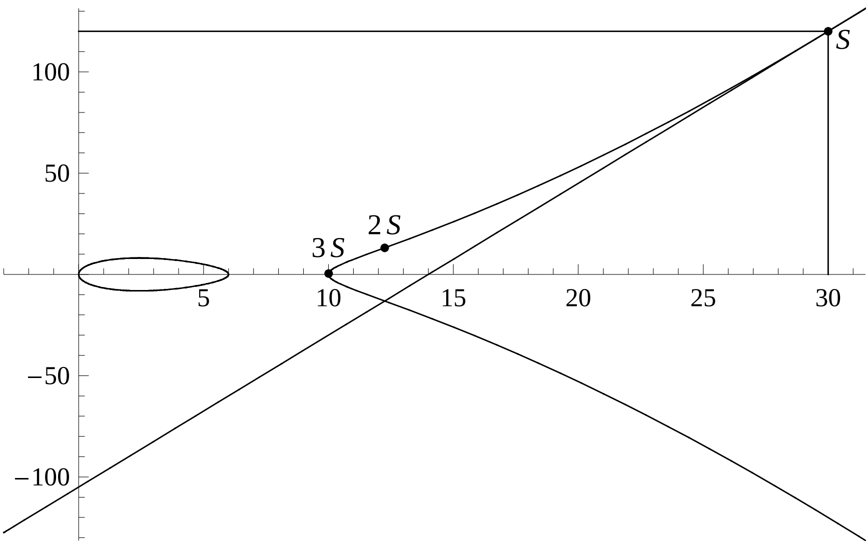
For the determination of $(x_3, -y_3)$, we just substitute $y = \lambda x + \mu$ in (2) to get $(\lambda x + \mu)^2 - x^3 - ax^2 - bx - c = 0$. But the expression on the left is a cubic in x with leading coefficient -1 and roots x_1, x_2, x_3. Hence

$$(\lambda x + \mu)^2 - x^3 - ax^2 - bx - c = -(x - x_1)(x - x_2)(x - x_3) = 0. \tag{3}$$

Equating coefficients of x^2 immediately gives

$$(x_3, y_3) \;=\; \left(\lambda^2 - a - x_1 - x_2,\; -\lambda x_3 - \mu\right), \tag{4}$$

our desired formula. Observe that if the line is vertical, we have $P_1 \oplus O = P_1 = O \oplus P_1$ and $(x, y) \oplus (x, -y) = O$, which suggests the notation $\ominus(x, y)$ for $(x, -y)$. As usual with Abelian groups, we write $2X$ for $X \oplus X$, and in general mX for $(m-1)X \oplus X$. An interesting alternative to (4), which has some merit when $c = 0$, is $(x_3, y_3) = \big((\mu^2 - c)/(x_1 x_2),\; -\lambda x_3 - \mu\big)$ obtained by equating the constants in (3).



Let S be the point $(30, 120)$ on $\mathcal{C}$. For $2S$, we put $a = -16$, $b = 60$, $c = 0$, $\lambda = 15/2$ and $\mu = -105$. Plugging these numbers into (4) gives $2S = (x_3, y_3) = (49/4, 105/8)$. We can then calculate $3S = 2S \oplus S$: $\lambda = 855/142$, $\mu = -4305/71$, leading to $3S = (50430/5041, 142680/357911)$ and another solution of (1), $P = 58$, $Q = 2911$, $R = 8487367$.

At any point on the curve of the form $(x, 0)$ the tangent is vertical and so $2(x, 0) = O$. Therefore points of order 2 occur at the roots of $x^3 + ax^2 + bx + c$, and when all three are present they together with O form a finite subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. From the picture we can identify rational points at $A = (0, 0)$, $B = (6, 0)$ and $C = (10, 0)$. Thus we have the 4×4 block on the left of the partial group addition table, below, where I have also included some combinations involving small multiples of S.

$\oplus$	O	A	B	C	S	$2S$	$3S$
O	O	A	B	C	$(30, 120)$	$\left(\frac{49}{4}, \frac{105}{8}\right)$	$\left(\frac{50430}{5041}, \frac{142680}{357911}\right)$
A	A	O	C	B	$(2, -8)$	$\left(\frac{240}{49}, -\frac{1800}{343}\right)$	$\left(\frac{10082}{1681}, -\frac{16472}{68921}\right)$
B	B	C	O	A	$(5, 5)$	$\left(\frac{54}{25}, \frac{1008}{125}\right)$	$\left(\frac{5}{841}, \frac{14555}{24389}\right)$
C	C	B	A	O	$(12, -12)$	$\left(\frac{250}{9}, -\frac{2800}{27}\right)$	$(10092, -1013028)$

The reader might like to spend some time using (4) to verify the entries. You can also confirm that each entry in the column headed S yields essentially the same solution of (1), and similarly for $2S$ and $3S$. With $(5, 5)$, for instance, $p = 1/2$, $r = -7/4$, and $Q = 2$ gives $P = 1$, $R = 7$.

By the Nagell–Lutz theorem [1, §II.5], a rational point (x, y) of finite order has integer coordinates, and if $y \neq 0$, then y^2 must divide the discriminant, $\Delta = 6^2 \cdot 10^2 \cdot 4^2 = 57600$. On checking each divisor of Δ, the only possible candidates are the eight points $(30, \pm 120)$, $(2, \pm 8)$, $(5, \pm 5)$, $(12, \pm 12)$. But they all become non-integral when doubled as can be seen from the table (e.g. $2(5, 5) = 2(B \oplus S) = 2B \oplus 2S = 2S$). So $\{O, A, B, C\}$ accounts for all rational points of finite order. Since S has infinite order, $\langle S \rangle$, the subgroup generated by S, is isomorphic to $\mathbb{Z}$. So together with the points of order 2 we have successfully identified the subgroup

$$G \;\cong\; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}.$$

The absence of any obvious candidate for a rational point not in G suggests that it is actually the whole group of rationals on $\mathcal{C}$. For a proof we use the methods of [1, Chapter III].

Let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + ax^2 + bx$ and let $\Gamma_{\mathcal{E}}$ be its group of rational points. The *rank* of $\mathcal{E}$ is the number of independent points of infinite order in $\Gamma_{\mathcal{E}}$. Define $\overline{\mathcal{E}}$, the *dual* of $\mathcal{E}$, by $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Applying the same process, $a \to -2a$ and $b \to a^2 - 4b$, to $\overline{\mathcal{E}}$ gives a curve which is isomorphic to $\mathcal{E}$ via the map $(x, y) \mapsto (x/4, y/8)$. The dual of $\mathcal{C}$ is

$$\overline{\mathcal{C}}: \quad y^2 \;=\; x^3 + 32x^2 + 16x.$$

For rational $z = r/s$, denote by $q(z)$ the *square-free kernel* of z. This is the number you get when you remove all squares from rs; so $q(-27/98) = -6$ for example. We use this function in the definition of the homomorphism

$$\alpha_{\mathcal{E}} : \Gamma_{\mathcal{E}} \;\to\; \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}, \qquad \begin{cases} \alpha_{\mathcal{E}}(O) \;=\; 1, \;\; \alpha_{\mathcal{E}}(0,0) \;=\; q(b), \\ \alpha_{\mathcal{E}}(x,y) \;=\; q(x) \text{ otherwise.} \end{cases}$$

Now we are ready to quote a formula from [1] for the rank r of $\mathcal{E}$:

$$2^{r+2} \;=\; |\alpha_{\mathcal{E}}(\Gamma_{\mathcal{E}})| \cdot |\alpha_{\overline{\mathcal{E}}}(\Gamma_{\overline{\mathcal{E}}})|. \tag{5}$$

It turns out that an element of $\alpha_{\mathcal{E}}(\Gamma_{\mathcal{E}})$ is a positive or negative square-free divisor d of b, and arises from the point $(dM^2/e^2,\; dMN/e^3)$ on $\mathcal{E}$, where (M, N, e) is an integer solution of

$$N^2 \;=\; dM^4 + aM^2e^2 + \frac{b}{d}\,e^4 \tag{6}$$

with $\gcd(M, e) = \gcd(N, e) = 1$. From the table on page 8 we can see that 1, 2, 3, 5, 6, 10, 15 and 30 belong to $\alpha_{\mathcal{C}}(\Gamma_{\mathcal{C}})$, accounting for all eight positive square-free divisors of 60. Since $\mathcal{C}$ does not exist to the left of the y axis, negative divisors can be ignored and hence $|\alpha_{\mathcal{C}}(\Gamma_{\mathcal{C}})| = 8$.

For $\overline{\mathcal{C}}$, the only square-free divisors of 16 are ± 1 and ± 2. However, by working modulo 8 (or otherwise) it can be shown that (6) with $a = 32$ and $b = 16$ has no admissible solution when $d = -1$ or ± 2. But $\alpha_{\overline{\mathcal{C}}}(O) = 1$. Therefore $|\alpha_{\overline{\mathcal{C}}}(\Gamma_{\overline{\mathcal{C}}})| = |\{1\}| = 1$. Putting this and $|\alpha_{\mathcal{C}}(\Gamma_{\mathcal{C}})| = 8$ into (5) yields $r = 1$. The problem is solved; $\mathcal{C}$ has rank 1 and

$$\Gamma_{\mathcal{C}} \;\cong\; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}.$$

---

[1] J. H. Silverman & J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

More identities involving partitions of an integer

Tommy Moorhouse

Introduction In this article we will denote by $Z_\xi(s)$ the generating function for partitions of integers into terms of the form $n = k_1\xi(p_{i_1}) + \cdots + k_r\xi(p_{i_r})$, where ξ is a function defined on the prime numbers (ordered by i with $p_1 = 2$). That is,

$$Z_\xi(s) = P_\xi(0) + P_\xi(1)e^{-s} + \cdots + P_\xi(k)e^{-sk} + \cdots,$$

where $P_\xi(n)$ is the number of partitions of n into integers of the given form. We have seen in previous articles (e.g. M500 **220**) that we can write

$$Z_\xi(s) \;=\; \prod_p \frac{1}{1 - e^{-s\xi(p)}}.$$

An identity We will make use of the identity for $t > 0$:

$$\frac{1}{1 - e^{-t}} \;=\; \prod_{j=0}^{\infty} \big(1 + \exp(-2^j t)\big).$$

This may be proved in several ways, one of which is to observe that the left-hand side is the sum $1 + e^{-t} + e^{-2t} + \cdots$ while the right-hand side is the generating function for partitions into distinct powers of 2. The product on the right-hand side converges since the terms tend to 1 as j tends to infinity. Now substitute $t = \xi(p)s$ and multiply over the primes p to find

$$Z_\xi(s) \;=\; \prod_p \frac{1}{1 - e^{-s\xi(p)}} \;=\; \prod_p \prod_{j=0}^{\infty} \big(1 + \exp(-2^j \xi(p)s)\big). \qquad (1)$$

Applications The rest of the article deals with specific functions ξ. As an elementary example, take $\xi(p_i) = 2i - 1$. The left-hand side of (1) is the partition function for partitions into odd integers, while it is easy to check that the right-hand side is that for partitions into distinct integers. This is another proof of this well-known result.

Now take n to be an odd integer and take $\xi(p_i) = n^{i-1}$. The left-hand side of (1) is the generating function for partitions into powers of n, while the right-hand side is that for partitions into distinct terms of the form $2^j n^k$. For example, if $n = 3$ the number of partitions of N into powers of 3 is equal to the number of distinct partitions into terms of the form $2^j 3^k$.

As a final example let $\xi(p_i) = 2^{i-1}$. The resulting partitions into powers of 2 are called binary partitions. Working from the product representation of $Z_\xi(s)$ we find the expression for $Z_\xi(s)$ to be

$$Z_\xi(s) \;=\; \prod_{j=0}^{\infty} \bigl(1 + \exp(-2^j s)\bigr)^{j+1}.$$

This leads to an expression for the number of binary partitions in terms of binomial coefficients, which it might be interesting to explore in a future article.

Notes Partitions into a class of integers where parts can be repeated (e.g. $7 = 3 + 3 + 1$) have something in common with elementary particles called bosons. Bosons can occupy the same state as other bosons in the same system (this lies behind the way lasers work). Here, two parts of the partition are in the state '3'. Partitions into distinct integers from a class have more in common with fermions, no two of which can be in the same state. This is the basis of the Pauli exclusion principle. What we have done above corresponds in a tongue in cheek way to the process of 'fermionization', a way of matching bosonic and fermionic descriptions of states in string theory.

Further reading Besides *The Theory of Partitions* by G. E. Andrews (Cambridge, 1984) and basic number theory texts like *Elementary Number Theory* by D. Burton (McGraw–Hill, 1995 (3rd Ed.)) and *Introduction to Analytic Number Theory* by T. Apostol (Springer, 1998) the reader with an inclination towards modern physics might be interested in parts of *A First Course in String Theory* by B. Zwiebach (Cambridge, 2009).

Problem 256.1 – Two bisextics

Tony Forbes

Two more equations for you to solve. As usual, exact expressions for the 12 roots are required in each case:

$$x^{12} + x^9 + 3x^7 - 1 \;=\; 0, \qquad\qquad x^{12} + 3x^5 - x^3 + 1 \;=\; 0.$$

We would also be interested if anyone knows the correct name for these things, or in general how to continue the sequence quadratic, cubic, quartic, quintic, sextic, septic, octic, ...

Problem 256.2 – Three rational numbers

Numbers $p + 2q$, pq^2 and $2pq + q^2$ are rational. Must p and q be rational?

Solution 254.1 – Four bottles

Find a two-variable function that provides a convincing model for the shape of the stretched plastic sheeting in this typical example of four one-litre bottles of fizzy stuff that I bought from my local supermarket.

Observe (for which I have no explanation) that the cross-section through the centre in the NW–SE direction, a parabola-like curve, differs from the NE–SW cross-section, which looks as if it could be a quartic with two local maxima and a local minimum at the central saddle point.

Ken Greatrix

Firstly, the shape of the plastic wrapping around the bottles. It would seem to me that the four bottles were placed in a short tube of shrink-wrap plastic. As the heat was applied, the open ends of the tube would give and allow the centre to dip. The circumference of the tube would not allow the same amount of shrinkage in the other direction. Had the process been done with a continuous tube or enclosed more bottles, the shape would (I think) have been more symmetrical. While shopping recently, I looked at a tray of a dozen small bottles for comparison, but the plastic wrapper wasn't tight enough to ascertain if this idea was correct.

For convenience, I rotate the photograph by 45° clockwise so that the lines drawn on the plastic become the x and y planes. To model the shape mathematically, I define a general equation for a quartic surface as

$$\begin{aligned} z &= a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 + b_0y^4 \\ &\quad + b_1y^3 + b_2y^2 + b_3y + b_4 + c_0x^4 + c_1x^3y + c_2x^2y^2 + c_3xy^3 + c_4y^4. \end{aligned}$$

In this expression c_0 and c_4 could be superfluous, but are included since the whole could have been compiled from three separate components. Also a_4 and b_4 could be reduced to a single constant relating to the height of the bottles. Any 1st or 3rd degree terms would make the result non-symmetrical, so their coefficients are zero.

From this full general formula I constructed a reduced general formula:

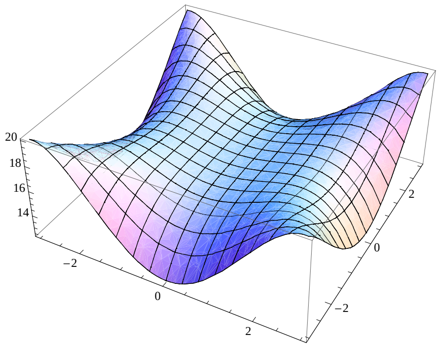
$$z = ax^4 + by^4 + cx^2 + dy^2 + ex^2y^2 + f,$$

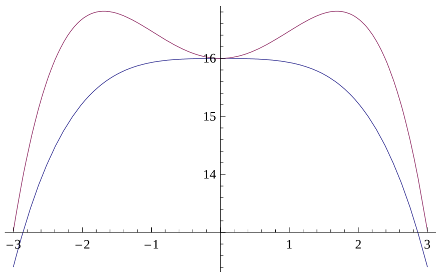
where a, b, c, d, e, f are constants.

When both x and y are 0, $z = f$; so this defines the height of the cross (assuming that zero height is the base of the bottles). When $y = 0$, $z = ax^4 + cx^2 + f$. To give a quartic shape, c is positive and a is negative. Similarly, when $x = 0$, $z = by^4 + dy^2 + f$. Since a parabolic shape is required, b, d are both negative.

After several attempts and a good few hours trying to solve the problem analytically, I resorted to a trial-and-error approach and I arrived at the following formula:

$$z = -0.1x^4 - 0.041y^4 + 0.57x^2 - 0.03y^2 + 0.13x^2y^2 + 16.$$





I think the root of my problem is that I have been trying 'force' a shape that probably doesn't fit the maths. If this is the case, although I have some workings-out that gave me the values of the coefficients (a, b, c, etc.), I couldn't model the complete surface. Perhaps there are too many values and not enough formulae to give the solution analytically.

Carrie Rutherford

Just a note to provide the Editor with some enlightenment. The difference between the NW–SE and NE–SW cross-section curves mentioned in the statement of the problem is easily explained. First the plastic sheeting is stretched over the bottles in one direction to create the vaguely parabolic curve. Then it is stretched in the other direction whereupon the quartic-like curve materializes.

Solution 250.4 – Divisor sum

Let k be a positive integer. Denote by $\sigma_k(n)$ the sum of the k^{th} powers of the (positive) divisors of n.

(i) Show that if $k \geq 2$ and $n^k + 1$ divides $\sigma_k(n)$, then n must be prime. For example, $\sigma_2(6) = 1^2 + 2^2 + 3^2 + 6^2 = 50$ is not divisible by $6^2 + 1 = 37$, but $\sigma_2(7)$, which is also equal to 50, is divisible by $7^2 + 1$, and hence 7 is prime.

(ii) Apart from the example above, are there any $k, n \geq 2$ for which $\sigma_k(n) = \sigma_k(n+1)$?

Reinhardt Messerschmidt

I will offer a solution to (i) and a partial solution to (ii). We first derive some inequalities that will be needed. If n is any positive integer, then

$$\begin{aligned}
\sigma_k(n) &\leq n^k + (n/2)^k + (n/3)^k + \cdots \\
&= n^k + (n/2)^k\big[1 + (2/3)^k + \cdots\big] \\
&\leq n^k + (n/2)^k\big[1 + (2/3)^2 + \cdots\big] \qquad \text{because } k \geq 2 \\
&= n^k + 4(n/2)^k\big[(1/2)^2 + (1/3)^2 + \cdots\big] \\
&= n^k + 4(n/2)^k\big[\pi^2/6 - 1\big] \\
&< n^k + 2.58(n/2)^k.
\end{aligned}$$

We will also use the cruder inequality

$$\sigma_k(n) \;<\; n^k + 2.58(n/2)^k \;\leq\; n^k + (2.58/4)n^k \;<\; 1.65n^k.$$

If n is odd, then

$$\begin{aligned}
\sigma_k(n) &\leq n^k + (n/3)^k + (n/5)^k + \cdots \\
&= n^k + (n/3)^k\big[1 + (3/5)^k + \cdots\big] \\
&\leq n^k + (n/3)^k\big[1 + (3/5)^2 + \cdots\big] \qquad \text{because } k \geq 2 \\
&= n^k + 9(n/3)^k\big[(1/3)^2 + (1/5)^2 + \cdots\big].
\end{aligned}$$

Now

$$(1/3)^2 + (1/5)^2 + \cdots \;=\; \left(\sum_{n\geq 1} n^{-2} - \sum_{n\geq 1} (2n)^{-2}\right) - 1 \;=\; 0.75(\pi^2/6) - 1,$$

therefore

$$\sigma_k(n) \;<\; n^k + 2.11(n/3)^k.$$

(i) If n^k+1 divides $\sigma_k(n)$, then it also divides $\sigma_k(n)-(n^k+1)$. We have

$$0 \;\le\; \sigma_k(n)-(n^k+1) \;<\; 1.65n^k-(n^k+1) \;<\; n^k+1,$$

therefore $\sigma_k(n)=n^k+1$, i.e. n is prime.

(ii) Suppose n is odd. Since $k\ge 2$ we have $(2.11)3^{-k}<2^{-k}$, therefore

$$\sigma_k(n) \;<\; n^k+2.11(n/3)^k \;<\; (n+1)^k+\big[(n+1)/2\big]^k \;<\; \sigma_k(n+1).$$

Suppose n is even. We have

$$\sigma_k(n)-\sigma_k(n+1) \;<\; n^k+2.58(n/2)^k-(n+1)^k \;=\; a_kn^k-(n+1)^k,$$

where $a_k=1+(2.58)2^{-k}$. We also have

$$\sigma_k(n)-\sigma_k(n+1) > n^k+(n/2)^k-(n+1)^k-2.11\big[(n+1)/3\big]^k = b_kn^k-c_k(n+1)^k,$$

where $b_k=1+2^{-k}$ and $c_k=1+(2.11)3^{-k}$. Let

$$r_k \;=\; \frac{1}{{a_k}^{1/k}-1}, \qquad s_k \;=\; \frac{1}{(b_k/c_k)^{1/k}-1}.$$

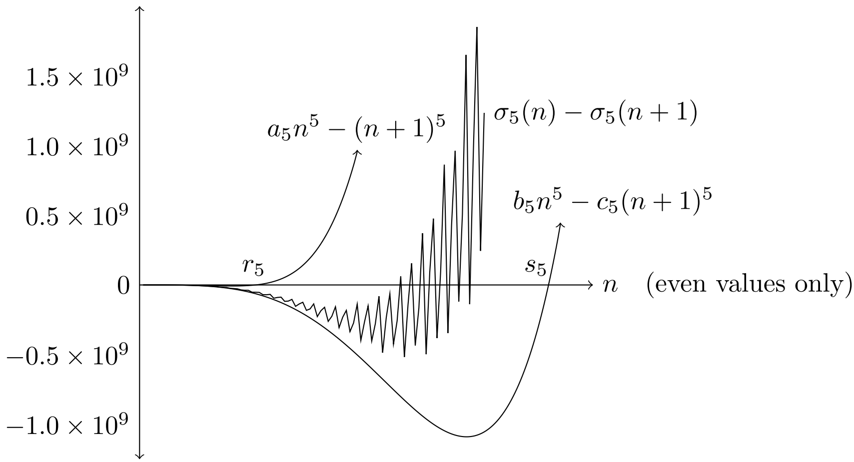
If $n\le r_k$ then $a_kn^k-(n+1)^k\le 0$, therefore $\sigma_k(n)-\sigma_k(n+1)<0$. If $n\ge s_k$ then $b_kn^k-c_k(n+1)^k\ge 0$, therefore $\sigma_k(n)-\sigma_k(n+1)>0$.

In summary, we have shown that if $k\ge 2$ and $\sigma_k(n)=\sigma_k(n+1)$, then n must be an even integer strictly between $\lfloor r_k\rfloor$ and $\lceil s_k\rceil$. The values of $\lfloor r_k\rfloor$ and $\lceil s_k\rceil$ for small k are as follows.

k	$\lfloor r_k\rfloor$	$\lceil s_k\rceil$
2	3	160
3	10	71
4	26	115
5	63	226
6	151	476

Given the large number of times that $\sigma_k(n)-\sigma_k(n+1)$ jumps between being negative and being positive in the interval $(\lfloor r_k\rfloor,\lceil s_k\rceil)$, it seems possible that it will land on 0 for more values of (k,n) than just $(2,6)$. $\square$

The graph shows the behaviour of $\sigma_5(n) - \sigma_5(n+1)$ for even n.



Solution 108.1 – Darts

> On a standard dartboard, what is the lowest total you can't score with one, two, three, ..., n darts?

David Wild

The lowest total one cannot score with one dart is 23. For $n \geq 2$ darts it will be shown that the first score which cannot be reached is $60(n-1)+43$.

If m, $m-1$, and $m-2$ can all be scored with n darts then, by throwing an appropriate treble, all the integers from $m+1$ to $m+60$ can be scored with $n+1$ darts. As we can score 20, 21, and 22 with one dart, up to 82 can be scored with two darts. Also we can score 38, 39, and 40 with one dart; so all the scores up to 100 can be reached with two darts. As $101 = 3 \cdot 17 + 50$ and $102 = 3 \cdot 20 + 3 \cdot 14$, all the numbers up to $102 = 60(2-1) + 42$ can be reached with two darts.

As 100, 101, and 102 can be scored with two darts, we can see all the numbers up to $162 = (3-1) \cdot 60 + 42$ can be reached with three darts. So in general we can reach all the numbers up to $(n-1) \cdot 60 + 42$ with n darts.

We now have to show that when $n >1$ we cannot reach $60(n-1)+43$. As $60(n-1)+43 > 60(n-1)+40$, all of the darts must score more than 40. Therefore each dart must score either 50 or a triple. As $60(n-1)+43 \equiv 1 \pmod 3$ at least two of the darts must score $50 \equiv 2 \pmod 3$. Since $50 \cdot 2 + (n-2) \cdot 60 = 60 \cdot (n-1) + 40 < 60 \cdot (n-1) + 43$ this is not possible.

Therefore the minimum score which cannot be reached with n darts is 23 when $n = 1$, and $60n - 17$ when $n > 1$.

Problem 256.3 – U-boat

Tony Forbes

A U-boat is constrained (by a damaged rudder perhaps) to moving in the x–z plane, $-300\,\mathrm{m} \le z \le 0\,\mathrm{m}$, with a top speed of $4\,\mathrm{m/s}$ in either direction. Fortunately you know where the (x, z) plane is, and the U-boat cannot outrun your destroyer's top speed of $10\,\mathrm{m/s}$. However, the ASDIC is not working; so the U-boat's x and z coordinates are not available. You can drop depth charges at a maximum rate of one per second. A hit anywhere in a box $80\,\mathrm{m} \times 20\,\mathrm{m} \times 20\,\mathrm{m}$ containing the entire submarine will put it out of action.

Devise a strategy for attacking the U-boat.

Problem 256.4 – Two septics

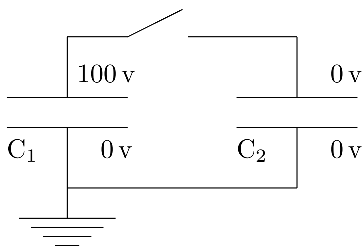
Tony Forbes

Two more equations for you to solve. Like the octics in M500 **254** and the bisextics in this issue they have only a few terms. As usual, exact expressions for the seven roots are required in each case:

$$x^7 + 7x^4 + 16 = 0, \qquad x^7 + x^6 + 3x^5 + 3 = 0.$$

Finding these things can be quite fun, too. At M500 we would be interested if you discover a 3- or 4-term equation of high degree that admits an exact solution but does not split into small polynomials with integer coefficients.

Problem 256.5 – Lost energy



Behold a simple circuit containing two capacitors of C farads each. The diagram represents the initial state, with 100 volts across C_1. When the switch is closed, current flows from C_1 to C_2. Thus C_1 loses charge to C_2 until they equalize at 50 volts across each capacitor.

Initially the total energy in the system is the $100^2C/2 = 5000C$ joules stored in C_1. But when the circuit has settled down after the switch is closed, the energy is split between the two capacitors at $50^2C/2$ joules each, making a total of $2500C$ joules. What has happened to the other $2500C$ joules?

Contents M500 256 – February 2014

04.00

Front cover: A *pancyclic* graph consisting of 40 vertices and 45 edges. Observe that a 3-cycle occurs at vertices (1, 2, 3) and a 4-cycle at (33, 34, 35, 36). Now see if you can find an example of a k-cycle for each of $k = 5$, 6, 7, ..., 40. (In case it's not clear from the picture, there really is an edge at {1, 3} and also at {33, 36}.)