2024-02-15

Euler's Prime-Producing Polynomial Revisited

Robert Heffernan

Nick Lord

Des MacHale

Euler's prime-producing polynomial revisited

ROBERT HEFFERNAN, NICK LORD, DES MacHALE

Introduction

Euler's polynomial $f(n) = n^2 + n + 41$ is famous for producing 40 different prime numbers when the consecutive values 0, 1, ..., 39 are substituted: see Table 1. Some authors, including Euler, prefer the polynomial $f(n-1) = n^2 - n + 41$ with prime values for $n = 1, \ldots, 40$. Since $f(-n) = f(n-1)$, $f(n)$ actually takes prime values (with each value repeated once) for $n = -40, -39, \ldots, 39$; equivalently the polynomial $f(n-40) = n^2 - 79n + 1601$ takes (repeated) prime values for $n = 0, 1, \ldots, 79$.

Euler introduced his polynomial in a brief remark at the end of a short letter to Johann Bernoulli III, [1], baldly stating: 'This progression 41, 43, 47, 53, … whose general term is $x^2 - x + 41$ is all the more remarkable because the first 40 terms are all prime numbers.' Incidentally, the 25th term of the progression is 641 – the prime factor that Euler used to show that the Fermat number $2^{32} + 1$ is composite.

In this paper, we take a closer look at Euler's polynomial for which, as above, we will reserve the notation $f(n)$ throughout.

n	$f(n)$	n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	10	151	20	461	30	971
1	43	11	173	21	503	31	1033
2	47	12	197	22	547	32	1097
3	53	13	223	23	593	33	1163
4	61	14	251	24	641	34	1231
5	71	15	281	25	691	35	1301
6	83	16	313	26	743	36	1373
7	97	17	347	27	797	37	1447
8	113	18	383	28	853	38	1523
9	131	19	421	29	911	39	1601

TABLE 1: The prime values of $f(n) = n^2 + n + 41$ for $n = 0, 1, \ldots, 39$.

The sequence of values of $f(n)$

In this section, we look at results which apply to the whole sequence of values $\{n^2 + n + 41 : n = 0, 1, 2, \ldots\}$.

- The occurrence of just 5 prime values guarantees that $x^2 + x + 41$ does not factorise over the integers.
  For if $x^2 + x + 41 = a(x)b(x)$, then $a(x) = \pm 1$, $b(x) = \pm 1$ have at most 4 solutions, and all other values of x would then give composite

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

values of $a(x)\,b(x)$. This idea is extended in [2]. Here, we could alternatively just observe that $x^2 + x + 41 = 0$ has no real roots because its discriminant is -163.

- Adjacent values $f(n-1), f(n)$ are coprime unless $n = 41k$ is a multiple of 41, when $\text{hcf}\big(f(41k-1), f(41k)\big) = 41$.
  For if $d \mid f(n-1), f(n)$, then d is odd and $d \mid f(n) - f(n-1) = 2n$. So $d \mid n$ and, since $d \mid f(n) = n^2 + n + 41$, we deduce that $d \mid 41$. Thus either $d = 1$ or $d = 41$; in the latter case, $n = 41k$ with $41 \mid f(41k)$ and $41 \mid f(41k-1)$.
  In particular, $f(41k)$ is composite for $k \geqslant 1$, so there are infinitely many composite values of $f(n)$. It is not known if there are also infinitely many prime values.
- The only value of n for which $f(n)$ is a square number is $n = 40$ when $f(40) = 41^2$. For if $n^2 + n + 41 = m^2$, then $4n^2 + 4n + 1 + 163 = 4m^2$, hence $4m^2 - (2n+1)^2 = 163$ so, by the difference of two squares, $2m - (2n+1) = 1$ and $2m + (2n+1) = 163$, from which $m = 41$ and $n = 40$.
  It is then natural to ask whether $f(n)$ is ever an odd power (greater than or equal to 3).
  If $f(n) = m^3$, then $n^2 + n + 41 = m^3$ from which $4m^3 - (2n+1)^2 = 163$. A solution thus corresponds to an integer point on the elliptic curve $4x^3 - y^2 = 163$. The *SageMath* mathematics software system, [3], confirms that there are no integer points on this curve.
  A computer search found no examples with $f(n) = m^k$ for $k = 5, 7, 9, 11$ and $n \leqslant 10^6$, which emboldens us to conjecture that $f(n)$ is never an odd power greater than 3.

In the next few sections, we will make repeated use of the following two key algebraic identities:

$$f(a+mb) = (a+mb)^2 + (a+mb) + 41 = f(a) + b\big[m^2 b + (2a+1)m\big], \quad (1)$$

with the special case that, if $b = f(a)$, then

$$f(a+mb) = b\big[1 + (2a+1)m + m^2 b\big]. \quad (2)$$

- The prime factors of $f(n)$ are necessarily greater than or equal to 41.
  Suppose, for contradiction, that $2 \leqslant p \leqslant 37$ is a prime such that $p \mid f(n)$.
  We can write $n = kp + r$ with $0 \leqslant r < p$. By (1), $f(r) = f(n - kp) = f(n) + p\big[k^2 p - (2n+1)k\big]$, hence p divides $f(r)$ and so has to coincide with one of the prime values $f(0), f(1), \ldots, f(p-1)$, which are all greater than or equal to $f(0) = 41$. This contradicts our initial assumption that $2 \leqslant p \leqslant 37$ and thus establishes the result.
- The number of distinct prime factors of $f(n)$ can be arbitrarily large.
  To see this, let $f(n) = k$. By (2), $f\big(n + k^2\big) = k\big[1 + (2n+1)k + k^3\big]$, with the two factors k, $1 + (2n+1)k + k^3$ being coprime. Thus $f\big(n + k^2\big)$ will have more distinct prime factors than $k = f(n)$.

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

We conjecture that, for each positive integer m, there is a value of n for which $f(n)$ has exactly m distinct prime factors; failing that, m possibly repeated prime factors. From the previous result we have the bound $n \geqslant 41^m$. The smallest such n for the first six values of m are listed below for the two cases of the conjecture.

$f(0) = 41$
$f(40) = 41^2, f(41) = 41 \times 43$
$f(420) = 47 \times 53 \times 71$
$f(1721) = 41^3 \times 43, f(2911) = 41 \times 47 \times 53 \times 83$
$f(14144) = 41 \times 47^4, f(38913) = 43 \times 47 \times 61 \times 71 \times 173$
$f(139563) = 41^4 \times 61 \times 113, f(707864) = 41 \times 43 \times 47 \times 53 \times 71 \times 1607$

- There are infinitely many primes for which $f(p)$ is composite.
  This result lies deeper since we need to invoke Dirichlet's theorem that, if a and b are coprime, then $a + nb$ is prime for infinitely many values of n.
  Let $1 \leqslant a \leqslant 39$. Then $f(a) = b$ is a prime number greater than $f(0) = 41$, so a and $b = a^2 + a + 41$ are coprime. By Dirichlet's theorem, there are infinitely many primes p of the form $p = a + nb$ for which, by (2), $f(p) = b\left[1 + (2a + 1)n + n^2 b\right]$ is composite.

Runs of prime and composite values of f (n)

In this section, we look at runs of prime and composite values of $f(n)$ for consecutive values of n.

- Composite values of $f(n)$ start to arise when we continue Euler's sequence of values beyond $n = 39$. A systematic way of listing some of them comes from (2),

  $$f(mb + a) = b\left[1 + (2a + 1)m + m^2 b\right] \text{ with } b = f(a),$$

  and its companion

  $$f(mb - a - 1) = b\left[1 - (2a + 1)m + m^2 b\right]$$

  where $b = f(-a - 1) = f(a)$ as well.
  These identities ensure that both $f(mb + a)$ and $f(mb - a - 1)$ are composite because they are multiples of $b = f(a)$. Thus, taking $a = 0, 1, 2, \ldots$ with corresponding $b = 41, 43, 47, \ldots$ (from Table 1), we see that $f(n)$ is composite when n has the following forms:

  $41m,\ 43m + 1,\ 47m + 2,\ 53m + 3,\ 61m + 4,\ 71m + 5,\ 83m + 6,\ 97m + 7, \ldots$

  $41m - 1,\ 43m - 2,\ 47m - 3,\ 53m - 4,\ 61m - 5,\ 71m - 6,\ 83m - 7,\ 97m - 8, \ldots$

  (These lists essentially coincide for $m = 1$, but not for $m \geqslant 2$.)
  In the range $40 \leqslant n \leqslant 100$, this gives the following values:
  $n = 40, 41, 44, 49, 56, 65, 76, 81, 82, 84, 87, 89, 91, 96$
  and, in fact, all other values of n in this range give prime values of $f(n)$.

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

The first composite value of $f(n)$ that does not arise from the lists above is $f(244) = 163 \times 367$, where neither 163 nor 367 is of the form $f(r)$.

One way of seeking such values is to start with one factor not of the form $f(r)$ such as $f(81) = 41 \times 163$. Then, applying (1), we see that 163 is always a factor of $f(163k + 81)$. Setting $k = 1, 2, \ldots$ in turn, we start to find suitable examples $f(244), f(407)$. Indeed, it is tempting to conjecture that there are infinitely many values of n not in the lists above that give rise to composite values of $f(n)$.

It is also well worth noting a striking sub-pattern visible in the first seven terms in the list of values of n in the range $40 \leqslant n \leqslant 100$ for which $f(n)$ is composite:

$f(40) = 41 \times 41$ (with two prime factors 0 apart)
$f(41) = 41 \times 43$ (2 apart)
$f(44) = 43 \times 47$ (4 apart)
$f(49) = 47 \times 53$ (6 apart)
$f(56) = 53 \times 61$ (8 apart)
$f(65) = 61 \times 71$ (10 apart)
$f(76) = 71 \times 83$ (12 apart).

This list suggests that $f\left(40 + k^2\right)$ is composite, indeed a product of two consecutive values of $f(n)$. This may be verified algebraically, as has been noted in the literature. From (1),

$$f\left(40 + k^2\right) = f(40) + k\left(k^3 + 81k\right) = k^4 + 81k^2 + 41^2 = \left(k^2 + 41\right) - k^2$$

$$= \left(k^2 - k + 41\right)\left(k^2 + k + 41\right) = f(k-1)f(k).$$

Hence, for $1 \leqslant k \leqslant 39$, $f\left(40 + k^2\right)$ factorises into the two prime values $f(k-1)$ and $f(k)$ with $f(k) - f(k-1) = 2k$. This pattern of composites thus persists as far as $f\left(40 + 39^2\right) = f(1561) = 1523 \times 1601$, but starts to fail after this: $f\left(40 + 40^2\right) = f(39) \times f(40) = 1601 \times 41^2$.

It is also worth noting that the identity $f\left(40 + k^2\right) = f(k-1)f(k)$ may be used to give alternative proofs to those above that there are infinitely many composite values of $f(n)$ and that the number of distinct prime factors of $f(n)$ can be arbitrarily large.

- Is there a run of m prime values of $f(n)$ for every $1 \leqslant m \leqslant 40$?
  Data such as that above for $n \leqslant 121$ shows that there are such runs for $1 \leqslant m \leqslant 8$ and $m = 10, 40$. Note that there cannot be a run of more than 39 primes after the initial run since $f(41k-1)$ and $f(41k)$ are both composite for $k \geqslant 1$. But this leaves the question about the remaining values of m and also whether the maximal run of 39 primes is ever achieved again.
- There are arbitrarily long runs of composite values of $f(n)$.
  Fix m and let $N = \operatorname{lcm}\{f(0), f(1), \ldots, f(m)\}$. Then, for $0 \leqslant k \leqslant m$, we have by (1), $f(N+k) = f(k) + N\left[N + (2k+1)\right]$. This is divisible by $f(k)$ and so is composite, giving a run of composites at least $m + 1$ long. But these runs of composites are slow to develop: the first run of two is

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

$f(40), f(41)$; of three is $f(121), f(122), f(123)$; and of four is $f(161), f(162), f(163), f(164)$.

- To investigate further how the prime and composite values of $f(n)$ are distributed, let $P(n)$ denote the number of prime values of $f(k)$ for $1 \leqslant k \leqslant n$, with $C(n)\big(= n - P(n)\big)$ similarly defined for the composite values. The long initial run of primes means that, envisaged as a race, $P(n)$ starts ahead of $C(n)$; the latter catches up at $n = 2336$. The lead then quickly changes hands several times (Figure 1) until $C(n)$ pulls ahead once $n \geqslant 2383$. On a large scale, shown in Figure 2, the graphs of $P(n)$ and $C(n)$ against perhaps suggest asymptotically linear behaviour, but we should be cautious for, while we know that $C(n) \to \infty$ as $n \to \infty$, it is very likely (but not proved) that $P(n) \to \infty$ as $n \to \infty$. Also, a conjecture due to Hardy and Littlewood ('Conjecture F', cited in [4]) is that $P(n) \sim C\dfrac{\sqrt{n}}{\ln n}$ for some constant C. If this is true, then $C(n) \sim n$ and the $P(n)$-line will gradually appear to flatten out.

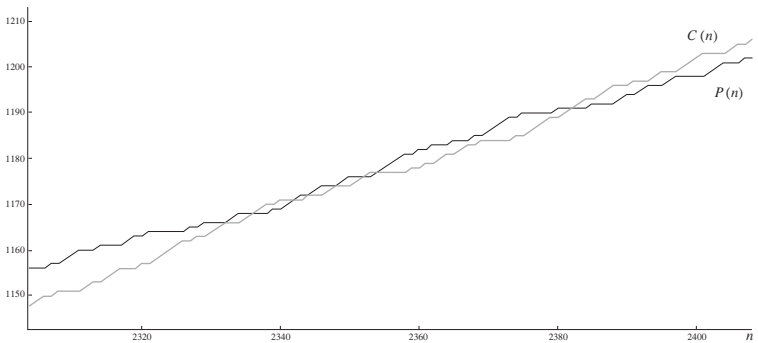

FIGURE 1: The portion of the race between $P(n)$ and $C(n)$ where the lead is exchanged several times.

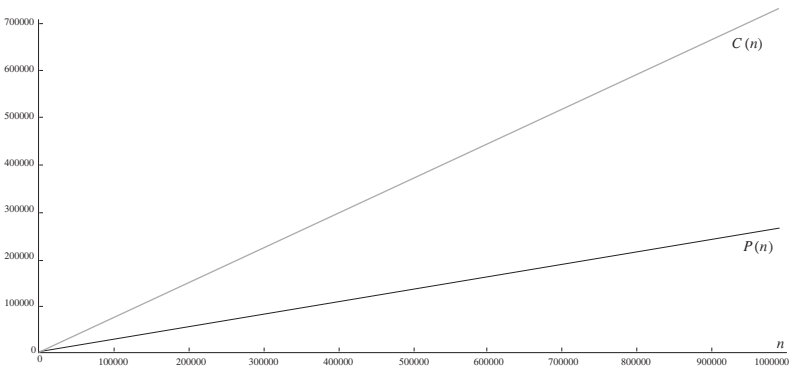

FIGURE 2: The race between $P(n)$ and $C(n)$ for values of n less than one million

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

- Other diagrams may also be used to show the prime-rich behaviour of Euler's polynomial. The *Ulam spiral*, [4], is a square spiral of the natural numbers where successive prime values of quadratic polynomials correspond to diagonal runs. Starting the spiral at 41, as in Figure 3, makes the long initial run of primes in Euler's polynomial strikingly apparent.

												71
												∧
57	<	56	<	55	<	54	<	53				70
∨								∧				∧
58		45	<	44	<	43		52				69
∨		∨				∧		∧				∧
59		46		**41**	>	42		51				68
∨		∨						∧				∧
60		47	>	48	>	49	>	50				67
∨												∧
61	>	62	>	63	>	64	>	65	>	66		

FIGURE 3: Ulam spiral starting at 41, displaying the values of $n^2 + n + 41$ on the '$y = x$' diagonal.

A variation on the Ulam spiral is the *Klauber triangle* in which successive prime values of quadratic polynomials show up as vertical runs. Starting the triangle at 41, as in Figure 4, again displays the prime values of Euler's polynomial in a very striking manner.

				41				
			42	43	44			
		45	46	47	48	49		
	50	51	52	53	54	55	56	
57	58	59	60	61	62	63	64	65

FIGURE 4: Klauber triangle starting at 41, displaying the values of $n^2 + n + 41$ on the central vertical line

An infinite series

Since $\dfrac{1}{n^2+n+41} < \dfrac{1}{n(n+1)}$ and $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n(n+1)}$ telescopes to a sum of 1, the series $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2+n+41}$ converges. We now evaluate this sum as a closed form using a method all the steps of which would have been familiar to Euler.

Logarithmic differentiation of the infinite product

$$\cos(\pi z) = \prod_{n=1}^{\infty}\left[1 - \frac{z^2}{(n-\frac{1}{2})^2}\right]$$

(which occurs in [5]) yields $\pi \tan(\pi z) = \displaystyle\sum_{n=1}^{\infty} \frac{2z}{(n-\frac{1}{2})^2 - z^2}$.

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

Substituting $z = \frac{1}{2}\sqrt{163}i$ then gives

$$\pi \tan\left(\frac{\pi\sqrt{163}}{2}i\right) = \sum_{n=1}^{\infty} \frac{\sqrt{163}i}{n^2 - n + 41},$$

so that

$$\sum_{n=1}^{\infty} \frac{1}{n^2 - n + 41} = \frac{\pi}{\sqrt{163}} \tanh\left(\frac{\pi\sqrt{163}}{2}\right).$$

But $\sum_{n=1}^{\infty} \frac{1}{n^2 - n + 41} = \frac{1}{41} + \sum_{n=1}^{\infty} \frac{1}{n^2 + n + 41}$, whence

$$\sum_{n=1}^{\infty} \frac{1}{n^2 + n + 41} = \frac{\pi}{\sqrt{163}} \tanh\left(\frac{\pi\sqrt{163}}{2}\right) - \frac{1}{41} \approx \frac{\pi}{\sqrt{163}} - \frac{1}{41}.$$

The latter is an astonishingly good approximation. Since

$$1 - \tanh x = \frac{2}{e^{2x} + 1} < 2e^{-2x},$$

the error is less than $\frac{\pi}{\sqrt{163}}\left[1 - \tanh\left(\frac{\pi\sqrt{163}}{2}\right)\right] < \frac{2\pi}{\sqrt{163}} e^{-\pi\sqrt{163}} \approx 1.9 \times 10^{-18}$.

There is an interesting alternative derivation of this approximation. Using the mid-ordinate approximation to the sum, in which the area, $\frac{1}{n^2 + n + 41}$, of the rectangle with base $n - \frac{1}{2} \leqslant x < n + \frac{1}{2}$ and height $\frac{1}{n^2 + n + 41}$ is approximated by $\int_{n-\frac{1}{2}}^{n+\frac{1}{2}} \frac{1}{x^2 + x + 41} dx$, we see that

$$\sum_{n=0}^{\infty} \frac{1}{n^2 + n + 41} \approx \int_{-\frac{1}{2}}^{\infty} \frac{1}{x^2 + x + 41} dx = \left[\frac{2}{\sqrt{163}} \tan^{-1} \frac{2x + 1}{\sqrt{163}}\right]_{-\frac{1}{2}}^{\infty} = \frac{\pi}{\sqrt{163}},$$

from which $\sum_{n=1}^{\infty} \frac{1}{n^2 + n + 41} \approx \frac{\pi}{\sqrt{163}} - \frac{1}{41}$.

Other properties of 41

The prime number 41 has featured prominently in this paper and, just for interest, we record some of its other special properties.

- 41 has the rare property of being a prime which is the sum of the first n primes, for $n = 6$.
- $p = 41$ is a *Sophie Germain prime* (one for which $2p + 1 (= 83)$ is also prime). As a result, $n = 41$ is also a *Curzon number* (one for which $(2n + 1) \mid (2^n + 1)$).
- 41 is the smallest positive integer whose reciprocal gives a repeating decimal of period 5: $\frac{1}{41} = 0.\dot{0}2439\dot{}$.
  This is because 41 divides $10^5 - 1 = 3^2 \times 41 \times 271$. In addition, an easy induction shows that 41 divides $\frac{1}{9}(10^{5k} - 1)$ which is the repunit 11…1 (with $5k$ ones).

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

- 41 is the smallest positive integer whose square root has a continued fraction of period 3: $\sqrt{41} = [6 : \dot{2}, \dot{2}, \dot{12}]$.
- 41 is the 5th centred square number, because $41 = 4^2 + 5^2$. As a consequence, (9, 40, 41) belongs to the $(2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1)$ family of primitive Pythagorean triples. It is also worth noting that setting $n = 50a + 20$ for $a \geqslant 0$ gives an infinite sequence of Pythagorean triples that end in 41, 40, 41: the first two such are (41, 840, 841) and (141, 9940, 9941).

Finally, relatively sophisticated algebraic number theory, [6], can be used to show that $n^2 + n + q$ cannot give prime values for all $0 \leqslant n \leqslant q - 2$ when $q > 41$. In fact, the only such values of q are 2, 3, 5, 11, 17, 41, so, for example $n^2 + n + 17$ is prime for all $0 \leqslant n \leqslant 15$. In this sense, Euler's polynomial is a champion prime-producing monic quadratic among those with negative discriminant. But there are quadratics with positive discriminant that produce longer runs of primes – for example, the Fung and Ruby polynomial $36n^2 - 810n + 2573$ which gives prime values for $0 \leqslant n \leqslant 44$, [7]. Also, the constant in Hardy and Littlewood's Conjecture F mentioned above depends on the coefficients of the quadratic involved and there are polynomials known with a higher constant than that for $n^2 + n + 41$. Thus, if Conjecture F is true, the values taken by such quadratics will appear relatively more prime-rich than the values taken by Euler's polynomial.

Acknowledgements

We are indebted to John Cremona, Michael Mardaus, Tobias Nagel and the other developers of the *SageMath* open-source software for analysing the properties of elliptic curves. We are also very grateful to the referee for a detailed and perceptive report which resulted in a considerably improved paper.

References

1. L. Euler, Extrait d'une lettre de M. Euler le pere à M. Bernoulli concernant le Mémoire imprimé parmi ceux de 1771 (1774) E461. English translation by Todd Doucet available at http://eulerarchive.maa.org/
2. N. Lord, Prime values of polynomials, *Math. Gaz.* **79** (November 1995) pp. 572-573.
3. SageMath, The Sage Mathematics Software System, Version 9.6 https://www.sagemath.org
4. Wikipedia article, *Ulam spiral*, accessed May 2023 at https://en.wikipedia.org/wiki/Ulam_spiral
5. L. Euler, *Introductio in analysin infinitorum*, vol 1 (1748) E101, chapter 9, accessed at http://eulerarchive.maa.org/

https://doi.org/10.1017/mag.2024.11 Published online by Cambridge University Press

6. H. Cohn, *Advanced number theory*, Dover (1980) pp. 155-158.
7. Wolfram mathworld, *Prime-generating polynomials*, accessed May 2023 at https://mathworld.wolfram.com/Prime-GeneratingPolynomial.html

10.1017/mag.2024.11

ROBERT HEFFERNAN
Department of Mathematics, Munster Technological University, Cork, Ireland
e-mail: *Robert.Heffernan@mtu.ie*
NICK LORD
Tonbridge School, Kent TN9 1JP
e-mail: *njl@tonbridge-school.org*
DES MacHALE
School of Mathematics, Applied Mathematics and Statistics, University College Cork, Cork, Ireland
e-mail: *d.machale@ucc.ief*

Problem Corner: Farewell to NJL

Nick Lord took over from the late Graham Hoare as the Editor of Problem Corner in July 2003. Graham had, as I said at the time, 'completed twenty years in harness'. Now Nick himself has decided to retire, having served his time for the same stretch. During this time he has supervised the selection of some 250 tantalising problems submitted by readers of the journal, as well as making apposite comments on solutions.

In 2008, Nick and Graham edited the book *'25 years of the Mathematical Gazette Problem Corner*'. A glance at the Index gives some idea of the variety and profundity of the themes explored, ranging from combinatorics, conics and constructions to polynomials, probability and packing problems. In the Editorial to the book, Nick observed that a published solution is never the final word on a problem. This is evident in the insight Nick has always displayed when discussing solutions, and his comments have often involved unexpected insights, impressive refinements and generalisations.

I am sure that Nick will continue to support the Problem Cornet by submitting new ideas and solutions, and maybe it will soon be time for a second edition of the compendium.

I am pleased to announce that Chris Starr will be the new Editor of Problem Corner, and know that he will have Nick's full support this role.

10.1017/mag.2024.12