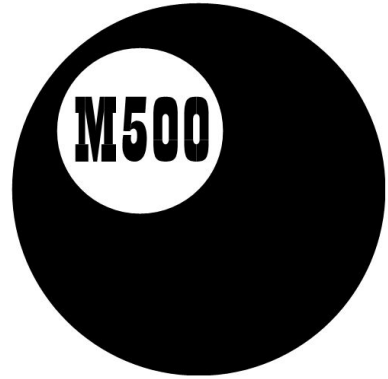


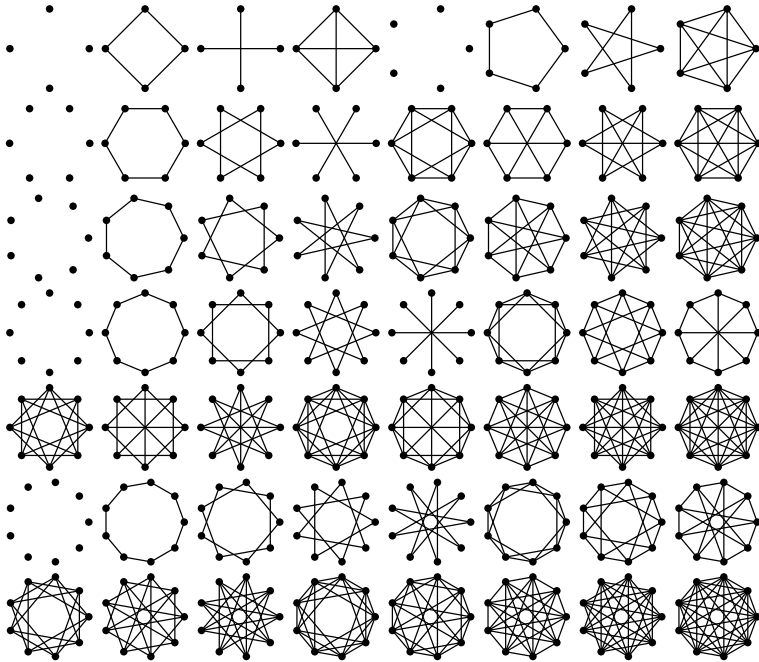


ISSN 1350-8539



# M500 285

---



---

## 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](http://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.

---

**Editor** – *Tony Forbes*

**Editorial Board** – *Eddie Kent*

**Editorial Board** – *Jeremy Humphries*

---

**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/](http://m500.org.uk/magazine/) from where a LaTeX template may be downloaded.

---

# Ramblings round representations – Part 2

## Roger Thompson

### 1 The proportion of $p_r$ with representations

Suppose there are  $C(N)$  (prime, root) combinations  $(p, r)$  for a particular  $f$  with  $p \leq N$ , and that  $R(N)$  of these have representations. Empirically,  $H = \lim_{N \rightarrow \infty} \frac{C(N)}{R(N)}$  exists and is an integer. As defined,  $H$  is specific to a particular polynomial. For each prime, this polynomial has a particular number of solutions of  $f(r) \equiv 0 \pmod p$ . We will call this its **root pattern**. We now consider all polynomials with the same root pattern as  $f$ , and see how  $H$  changes. Our general polynomial is

$$f = X^3 + PX^2 + QX + R.$$

If  $P = 3M + N$ , we can make the substitution  $X = Y - M$  to give

$$g(Y) = Y^3 + P'Y^2 + Q'Y + R',$$

where  $0 \leq P' \leq 2$ . If  $P' = 2$ , we can make the substitution  $Y = -Z - 1$  to give

$$h(Z) = Z^3 + Z^2 + (Q' - 1)Z + Q' - R' - 1.$$

These substitutions do not change  $H$  since they apply directly to roots and representations. The substitutions also leave the value of the discriminant unchanged.

If we generalize the substitution to  $Z = \frac{aX^2 + bX + c}{k}$ , can we make other monic polynomials  $Z^3 + hZ^2 + iZ + j \pmod f$  with integer coefficients? The answer seems to be sometimes. The underlying algebra is revolting (see Appendix); so I have had to use trial and error to search for solutions. It is therefore dubious to claim that no solutions exist for particular polynomials. Where solutions are found, the root pattern is unchanged, but the discriminant and number of prime representations for each  $p$  may change, hence  $H$  may change. To illustrate, we consider the following six polynomials.

Polynomial	$H$	Real root
$X^3 + 126$	27	$\alpha = -5.0132979349645845$
$X^3 - 126X + 714$	18	$\beta = -13.391016663204642$
$X^3 + 126X + 462$	18	$\gamma = -3.3644207932754719$
$X^3 + 252X - 420$	18	$\delta = 1.648877141689113$
$X^3 - 252X + 1596$	18	$\varepsilon = -18.404314598169226$
$X^3 + 756X + 1302$	27	$\zeta = -1.7155436515863585$

The above polynomials have a distinct but possibly overlapping set of primes with representations even if they share the same  $H$  value.

The class number described in standard textbooks on algebraic number theory, traditionally denoted by  $h$ , is an integer, and is the same for all polynomials with the same root pattern (for example,  $h = 9$  for the above polynomials). Just as  $H$  could be defined as the proportion of ideals of the form  $\langle X - r, p \rangle$  that are principal, so  $h$  is defined as the proportion of fractional ideals that are principal. Informally, fractional ideals can be thought of as ordinary ideals with each element divided by some fixed polynomial with integer coefficients. This is equivalent to multiplying by some fixed polynomial and dividing by an integer (Part 3 will explain this). Standard theory uses fractional ideals to define inverses of ideals, which then gives rise to the nice group properties that result in  $h$  being an integer. Calculation of the class number for a particular root pattern is far from trivial, and requires a good deal of theory. (See [Barrucand *et al.* (1976)] and [Cohen (2000)] for details.)

Without delving into such theory, can we derive  $h$  just from the properties of prime representations? It would appear that  $H$  is always a multiple of  $h$ , and that  $h = \text{gcd}(\{H\})$  for all polynomials with the same root pattern. It is worth observing that I have found no examples of polynomials with an apparently unique root pattern for which  $H \neq h$ , so perhaps the trial and error search was adequate after all. If several polynomials with the same root pattern are found, establishing a set with different  $H$  values can be very time consuming. What can we learn from analysis of a single polynomial? To explore this, we will look further into the relationships between the six polynomials above. The tables below show how the roots relate to each other numerically.

$\alpha$	$\beta$	$\gamma$
$\alpha$	$-\alpha^2 + 3\alpha$	$-\alpha^2 - 3\alpha$
$\alpha$	$3$	$3$
$-\beta^2 - 3\beta + 84$	$\beta$	$2\beta^2 + 17\beta - 168$
$11$	$-2\gamma^2 + 11\gamma - 168$	$11$
$-\gamma^2 - 3\gamma - 84$	$17$	$\gamma$
$17$	$-3\delta^2 + 2\delta - 504$	$-\delta^2 + 26\delta - 168$
$-\delta^2 - 12\delta - 168$	$38$	$38$
$\varepsilon^2 + 12\varepsilon - 168$	$-\varepsilon^2 - 2\varepsilon + 168$	$-3\varepsilon^2 - 26\varepsilon + 504$
$38$	$10$	$10$
$-2\zeta^2 - 27\zeta - 1008$	$-5\zeta^2 + 29\zeta - 2520$	$-\zeta^2 + 83\zeta - 504$
$193$	$193$	$193$

$\delta$	$\varepsilon$	$\zeta$
$\frac{-\alpha^2 - 6\alpha}{3}$	$\frac{-\alpha^2 + 6\alpha}{3}$	$\frac{-2\alpha^2 - 9\alpha}{3}$
$\frac{3\beta^2 + 20\beta - 252}{11}$	$\frac{-\beta^2 + 8\beta + 84}{11}$	$\frac{5\beta^2 + 37\beta - 420}{11}$
$\frac{\gamma^2 + 20\gamma + 84}{17}$	$\frac{-3\gamma^2 + 8\gamma - 252}{17}$	$\frac{\gamma^2 + 37\gamma + 84}{17}$
$\delta$	$\frac{-2\delta^2 - 5\delta - 336}{19}$	$\frac{-\delta^2 + 64\delta - 168}{38}$
$\frac{-2\varepsilon^2 - 19\varepsilon + 336}{5}$	$\varepsilon$	$\frac{-7\varepsilon^2 - 64\varepsilon + 1176}{10}$
$\frac{\zeta^2 + 110\zeta + 504}{193}$	$\frac{-7\zeta^2 + 2\zeta - 3528}{193}$	$\zeta$

We will call the denominator associated with a particular polynomial its **fractional constant**. Where do these fractional constants come from? Factoring the discriminants reveals all!

Polynomial	Discriminant $\Delta$
$X^3 + 126$	$-2^2 3^5 7^2 \times 3^2$
$X^3 - 126X + 714$	$-2^2 3^5 7^2 \times 11^2$
$X^3 + 126X + 462$	$-2^2 3^5 7^2 \times 17^2$
$X^3 + 252X - 420$	$-2^2 3^5 7^2 \times 2^2 19^2$
$X^3 - 252X + 1596$	$-2^2 3^5 7^2 \times 2^2 5^2$
$X^3 + 756X + 1302$	$-2^2 3^5 7^2 \times 193^2$

It is clearly necessary to find a reasonable number of different polynomials with the same root pattern in order to distinguish the invariant part of the discriminant from the fractional constant part, and to ensure that examples are found such that  $\text{gcd}(\text{root relation numerator coefficients, fractional constant}) = 1$ .

Using  $\xi = X^3 + 126$  to identify the root pattern common to the above polynomials, the primes 1499, 1709, 2351 and 3373 (chosen at random) have 1, 1, 1 and 3 solutions respectively of  $\xi(r) \equiv 0 \pmod p$ . The following table shows how many of these have representations.

Polynomial	1499	1709	2351	3373
$X^3 + 126$	0	1	0	0
$X^3 - 126X + 714$	1	1	0	3
$X^3 + 126X + 462$	1	0	0	3
$X^3 + 252X - 420$	1	1	1	1
$X^3 - 252X + 1596$	0	1	1	3
$X^3 + 756X + 1302$	0	0	1	1

To see why these differences occur, we will see how the representations in the six different polynomials may relate to each other. We will use  $\rho_{(f)}$ ,  $N_{(f)}$ , etc. to make it clear which polynomial the representation or norm refers to. For  $f = X^3 + 126$ ,

$$\rho_{(f)}(1709_{251}) = X^2 - 6X + 29.$$

For  $g = Y^3 - 126Y + 714$ ,

$$\rho_{(g)}(1709_{898}) = 1156Y^2 - 15480Y + 61637,$$

where  $Y = \frac{-X^2 + 3X}{3}$ . Here we are treating the relation between the numeric roots  $\alpha, \beta$  defined above algebraically. If we evaluate  $1156Y^2 - 15480Y + 61637 \pmod f$ , we find that the denominator of  $3^2$  gets cancelled out of the resulting coefficients, giving

$$\begin{aligned} 1156Y^2 - 15480Y + 61637 &\equiv 6316X^2 - 31664X + 158741 \\ &\equiv \rho_{(f)}(1709_{251})U_1^2 \pmod f, \end{aligned}$$

where  $U_1 = -X^2 + 5X - 25$  is a unit. In other words, the representations are really invariant. While this convenient cancellation occurs for all  $\rho_{(f)}$ ,  $\rho_{(g)}$  using the above  $f, g$ , it does not happen for all  $f, g$ . For example, if we use

$$f = X^3 - 126X + 714 \text{ and } g = Y^3 + 126,$$

we get

$$X^2 - 6X + 29 \equiv \frac{3Y^2 - 24Y + 67}{11} \pmod g.$$

The remedy for this will turn out to be very useful (see the next section).

If we continue to use  $f = X^3 + 126$ , we can see why  $h = Z^3 + 126Z + 462$  has no representation for 1709<sub>396</sub>. We have  $X = (-Z^2 - 3Z - 84)/17$  from the table of root relations, above. If we evaluate  $X^2 - 6X + 29 \pmod h$ , we get  $(9Z^2 - 24Z + 1249)/17$ , with

$$N_{(h)}(9Z^2 - 24Z + 1249) = 17^3 1709,$$

as expected. Since the coefficients must be integers, this fractional representation is not allowed. Let's see what happens if we change this. We will call a polynomial  $g$  with fractional constant  $k$  such that  $g(r) \equiv 0 \pmod p$  and  $N(g) = k^3 p$  a **fractional representation** of  $p_r$ , denoting  $\frac{g}{k}$  by  $\rho_k(p_r)$ .

Repeating the above table for fractional representations, we have the following.

Polynomial	1499	1709	2351	3373
$X^3 + 126$	1	1	1	3
$X^3 - 126X + 714$	1	1	1	3
$X^3 + 126X + 462$	1	1	1	3
$X^3 + 252X - 420$	1	1	1	3
$X^3 - 252X + 1596$	1	1	1	3
$X^3 + 756X + 1302$	1	1	1	3

This identical tally is true for all (prime, root) combinations for any of the six polynomials listed, so that their fractional representations each have  $H = 9 = h$ . This is not true in general. For example,  $X^3 - 252X + 4830$  has  $H = 9$ , but its fractional representations have  $H = 3$ . In the next section we will see how to remedy this.

## 2 Units and fractional representations

Every integer representation has a fractional representation, formed simply by multiplying coefficients by the fractional constant  $k$ . Fractional representations may also take other forms. This section identifies methods for determining whether these forms can be converted into integer representations, and if so, doing the conversion. To illustrate, we use

$$f = X^3 - 252X + 4830,$$

which has fractional constant  $k = 109$ . This is chosen because its units have large magnitude, as we shall see shortly, so that many integer representations of small primes have large magnitude. In such cases, we are likely to find forms such that the coefficients of their numerators are not all divisible by  $k$ . To find fractional representations, we can use the  $\mu, \nu$  parameters of Part 1 section 2, searching for quadratics having numerators with norm  $k^3 p$ , and **fractional units** (quadratics with numerator norm  $k^3$ ), which we will label  $V_1, V_2$ . In our case, we find that

$$V_1 = 7X^2 - 153X + 1549 \quad \text{and} \quad V_2 = 2X^2 + 3X - 881$$

(so that  $V_1 V_2 \equiv 109^2 \pmod{f}$ ). If  $F$  is  $V_1, V_2$  or the numerator of any  $\rho_{k(f)}$ , we find that the coefficients of  $V_i F$  are congruent to  $kG \pmod{f}$  for some quadratic  $G$  with integer coefficients. In other words,  $\frac{F V_i^n}{k k^n} \equiv \frac{G}{k} \pmod{f}$  for any  $n$ . This is true for any  $f$ .

If the coefficients of  $(V_i/k)^n \pmod{f}$  are all divisible by  $k$  for some  $n$ , we have found a unit. In our case, we find this is true for  $n = 108$ , i.e.  $(V_i/109)^{108} \equiv U_i \pmod{f}$ , giving

$U_1 = 3658104367599407843493041112227448656853402355062668975554$   
 $841209590218208715112793914620303079596702495384082670977127572$   
 $626229212524864793318034959086580656131176365683172738170548506$   
 $0303401456905770X^2$   
 $- 7963230601255965147963325218122021385203847435815852147296301$   
 $638850108197010770161153838456295378253945850474118533522671473$   
 $402403926983057602809655959466730583952415420591462995339852168$   
 $14453120236530X$   
 $+ 8116522975629108512262155029009467050333391167755050694009672$   
 $374521320789728445988865599133949170067447537113569253277853315$   
 $574658639013778189027548303186762591673432575038446702945134775$   
 $812212378553641,$

$U_2 = -223213534699484767598556868694248198054880466122976214252$   
 $738963375074934119457407146093130822778470X^2$   
 $+ 3176600891668783130893259878088396769848544731511149096559585$   
 $585594937286287006231348252264827998730X$   
 $+ 1749265320582681358893780014909843966934656755319684223776177$   
 $59766299474063505786399408550940773267961.$

For an example that does convert into an integer representation, we use

$$\rho_{109}(587_{543}) = \frac{-X^2 - 56X + 59}{109}.$$

We find that

$$(-X^2 - 56X + 59) \left( \frac{V_2}{109} \right)^5 \equiv 109(-1157X^2 - 17609X + 164951) \pmod{f};$$

so

$$\rho(587_{543}) = -1157X^2 - 17609X + 164951.$$

A very small proportion of representations cannot be derived in this way. For example, for

$$\xi = X^3 + 756X + 1302,$$

which has fractional constant 193, we have

$$\begin{aligned} V_1 &= 19X^2 - 33X + 14401, \\ V_2 &= 2X^2 + 27X + 43, \\ (V_i/193)^{64} &\equiv U_i \pmod{\xi}, \\ \rho(46549_{9167}) &= -39966019177047621360551793135X^2 \\ &\quad - 1371904296522449188743007912428X \\ &\quad - 2235938114284126051579194454271, \end{aligned}$$



and

$$\rho_{193}(46549_{9167}) = 17X^2 + 30X + 16981,$$

but there is no  $n$  for which

$$\rho_{193}(46549_{9167})(V_i/193)^n \equiv \rho(46549_{9167}) \pmod{\xi}.$$

I haven't found sufficient examples to study these exceptions systematically.

Now we will see how to convert a fractional representation in one polynomial to an integer representation in another with the same root pattern, even if an integer representation doesn't exist in the first one. We will use

$$g = Y^3 + 126, \quad f = X^3 - 252X + 4830,$$

as above. Using the techniques of the previous section, we have

$$X = \frac{-2Y^2 + 3Y}{3}, \quad Y = \frac{-2X^2 - 3X + 336}{109}.$$

We find

$$\rho_{3(g)}(4451_{2611}) = \frac{-Y^2 + 30Y + 177}{3}.$$

Substituting for  $Y$  and working modulo  $f$ , we get

$$\rho_{109(f)}(4451_{3685}) = \frac{-19X^2 + 26X + 9623}{109}.$$

The root

$$3685 \equiv (-2r_g^2 + 3r_g)3^{-1} \equiv 1484(-2r_g^2 + 3r_g) \pmod{4451},$$

where  $r_g = 2611$ . We find

$$\begin{aligned} & \frac{-19X^2 + 26X + 9623}{109} (V_2/109)^{43} \\ & \equiv -5670888303188440227230424943465190306088X^2 \\ & \quad - 42392407415457568754374927553589379742737X \\ & \quad + 1764479203440589754949545207687502079571057 \pmod{f} \\ & = \rho_{(f)}4451_{3685}. \end{aligned}$$

The polynomial  $f = X^3 + 1719$ , with real root  $\alpha$ , has  $H = 102$  and has fractional constant 3. Its fractional representations have  $H = 34 = h$ . The polynomial

$$g = X^3 + 6876X + 573$$

has real root  $\beta$ , with

$$\beta = \frac{\alpha^2 + 12\alpha}{3}, \quad \alpha = \frac{-\beta^2 + 48\beta - 4584}{383}.$$

However, a negligible number of fractional representations in  $f$  convert to integer representations in  $g$ . In fact,  $H = 384 \times 34 = 13056$  for  $g$ .

### 3 The three root case

The congruence  $f \equiv 0 \pmod p$  has three roots for around one sixth of primes. If  $i, j, k$  are three roots of  $f \equiv 0 \pmod p$ , then from Part 1 section 3, we have  $\rho(p_i)\rho(p_j)\rho(p_k) = p$ . If two representations are known to exist, then the third one can be calculated from this equation, so apart from the special case of  $p = 2$ , there are no primes with two representations.

We might suppose for such primes that the proportion of (prime, root) combinations with representations is the same as that for all (prime, root) combinations, i.e.  $1/H$ . This is indeed so. Let  $T_i$  denote the proportion of primes with three roots such that  $i$  of the roots have representations. We have already seen that  $T_2 = 0$ . We therefore have

$$\frac{0 \times T_0 + 1 \times T_1 + 3 \times T_3}{3(T_0 + T_1 + T_3)} = \frac{1}{H}.$$

Intriguingly, the ratios  $T_0 : T_1 : T_3$  seem to be constrained further than the requirements of the above equation. Empirically,

$$T_0 : T_1 : T_3 = \frac{H^2 - 3H}{3^n} + 2 : \frac{3H}{3^n} - 3 : 1$$

for some  $n \geq 0$  (specific to  $f$ ) such that  $H$  is divisible by  $3^n$ .

Consider the primes for which  $f \equiv 0 \pmod p$  has three roots, and all three have representations. If

$$f = X^3 + 6876X + 573$$

for example, there are 580 such primes less than  $6.25 \times 10^{12}$ . For this polynomial and a few others, the three representations differ only in one of the coefficients of  $X^2, X^1, X^0$  for a significant proportion of such primes. Here, 336 have representations that differ only in the coefficient of  $X$ , e.g.

$$\begin{aligned} \rho(142582933_{91094652}) &= -36X + 13, \\ \rho(142582933_{74261944}) &= 48X + 13, \\ \rho(142582933_{119809270}) &= 144X + 13, \end{aligned}$$

and another 20 that differ only in the coefficient of  $X^2$ , e.g.

$$\begin{aligned}\rho(197047927801_{147909160322}) &= 30X^2 + 2907X + 244, \\ \rho(197047927801_{176396834604}) &= -40X^2 + 2907X + 244, \\ \rho(197047927801_{69789860676}) &= -242X^2 + 2907X + 244.\end{aligned}$$

This constrains the sum of the variable coefficients. For example, if  $a, b$  are the fixed coefficients of  $X^2, X$ , then the sum of the variable coefficients must be  $bP + 2aQ - aP^2$ . Further constraints arise since the norms of any two of the representations must be equal, and the product of all three is  $p \times U_i^n$ . However, the thicket of algebra that results seems particularly impenetrable!

#### 4 (Prime, root) combinations without representations for class 1 polynomials

From the definition of  $H$ , it is not clear whether for  $H = 1$ , there are a finite number of (prime, root) combinations without representations. We will state (but not prove) that this is so, and that all such primes are divisors of the discriminant of  $f$ . Examples:

$X^3 + X^2 + X + 250$  has a representation for every (prime, root) combination except  $17_3$  (a repeated root), and

$$\Delta(X^3 + X^2 + X + 250) = -1684003 = -17^2 5827;$$

$X^3 + X^2 + 8X - 17$  has a representation for every (prime, root) combination except  $23_{15}$ , and

$$\Delta(X^3 + X^2 + 8X - 17) = -12167 = -23^3;$$

$X^3 + X^2 + 31$  has a representation for every (prime, root) combination except  $29_9$  (a repeated root), and

$$\Delta(X^3 + X^2 + 31) = -26071 = -29^2 31;$$

$X^3 + X^2 + 17X + 13$  has a representation for every (prime, root) combination except  $2_1$  and  $5_3$ , and

$$\Delta(X^3 + X^2 + 17X + 13) = -20000 = -2^5 5^4.$$

By changing the discriminant, other polynomials with the same root pattern may remedy this deficiency. For example, we can use the techniques in

section 1 to transform  $X^3 + X^2 + X + 250$  into  $X^3 + X^2 + 9X - 8$ . This has discriminant  $-5827$ , and as expected, the three roots  $17_5, 17_{12}, 17_6$  all have representations.

### 5 Part 3

Part 3 is concerned with techniques for finding representations, and selecting polynomials for which these techniques are most effective.

### 6 Appendix

#### Generalizing polynomials with a specific root pattern

Given

$$f = X^3 + PX^2 + QX + R = 0$$

with discriminant  $\Delta$ , we want to find

$$Z^3 + hZ^2 + iZ + j \equiv 0 \pmod{f} \quad \text{with} \quad Z = \frac{aX^2 + bX + c}{k},$$

where  $a, b, c, h, i, j, k$  are integers. Let

$$mX^2 + nX + t \equiv (aX^2 + bX + c)^2 \pmod{f},$$

$$uX^2 + vX + w \equiv (aX^2 + bX + c)^3 \pmod{f}.$$

Then

$$m = 2ac + b^2 - a^2Q - 2abP + a^2P^2,$$

$$n = 2bc - a^2R - 2abQ + a^2PQ,$$

$$t = c^2 - 2abR + a^2PR,$$

$$\begin{aligned} u &= 3ac^2 - 3a^2bR + 2a^3PR + 3b^2c - 3ab^2Q + 6a^2bPQ - 3a^2cQ \\ &\quad - 6abcP + 3a^2cP^2 + a^3Q^2 - 3a^3P^2Q - b^3P + 3ab^2P^2 \\ &\quad - 3a^2bP^3 + a^3P^4, \end{aligned}$$

$$\begin{aligned} v &= 3bc^2 - 3ab^2R + 3a^2bPR - 3a^2cR - 6abcQ + 3a^2cPQ + 2a^3QR \\ &\quad - a^3P^2R + 3a^2bQ^2 - 2a^3PQ^2 - b^3Q + 3ab^2PQ \\ &\quad - 3a^2bP^2Q + a^3P^3Q, \end{aligned}$$

$$\begin{aligned} w &= c^3 - 6abcR + 3a^2cPR + a^3R^2 + 3a^2bQR - 2a^3PQR - b^3R \\ &\quad + 3ab^2PR - 3a^2bP^2R + a^3P^3R. \end{aligned}$$

We require

$$hk = \frac{bu - av}{an - bm}, \quad ik^2 = \frac{vm - un}{an - bm}, \quad jk^3 = -w - hkt - ik^2c.$$

Some indication as to why factors of the discriminant are involved in the denominator can be derived from the section ‘Algebraic integers and  $f'(X)$ ’ in M500 **276**. This gives the following:

$$\frac{1}{f'(X)} \equiv AX^2 + BX + C \pmod{f},$$

where

$$A = \frac{2P^2 - 6Q}{\Delta}, \quad B = \frac{2P^3 - 7PQ + 9R}{\Delta}, \quad C = \frac{P^2Q - 4Q^2 + 3PR}{\Delta};$$

$$\frac{X + P}{f'(X)} \equiv BX^2 + EX + F \pmod{f},$$

where

$$E = \frac{2P^4 - 8P^2Q + 2Q^2 + 12PR}{\Delta}, \quad F = \frac{P^3Q - 4PQ^2 + P^2R + 6QR}{\Delta};$$

$$\frac{X^2 + PX + Q}{f'(X)} \equiv CX^2 + FX + I \pmod{f},$$

where

$$I = \frac{P^2Q^2 - 4Q^3 + 10PQR - 2P^3R - 9R^2}{\Delta}.$$

## Problem 285.1 – Roots

Suppose  $r > 0$  and for positive integer  $m$ , define

$$F(m, r, x) = \frac{\sum_{i=0}^{m/2} \binom{m}{2i} r^i x^{m-2i}}{\sum_{i=0}^{m/2} \binom{m}{2i+1} r^i x^{m-2i-1}}.$$

Show that

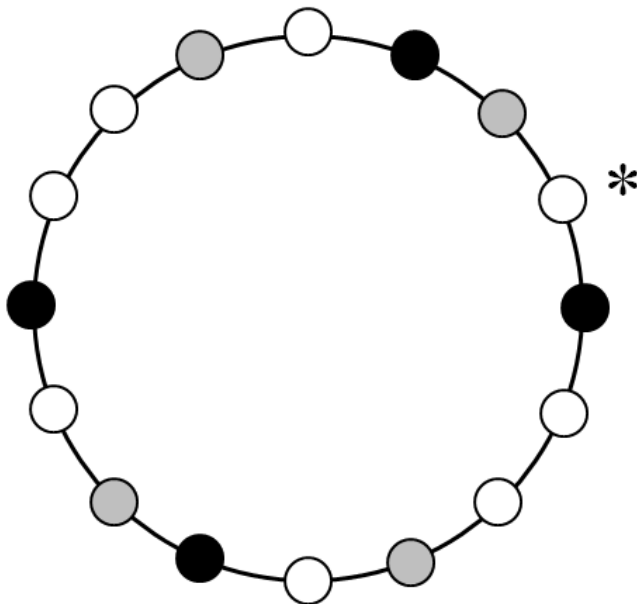
$$F(m, r, 1) \rightarrow \sqrt{r} \quad \text{as } m \rightarrow \infty.$$

For example,  $F(20, 5, 1) = 2.2360679970\dots$ , giving  $\sqrt{5}$  to 7 decimal places. Moreover, if you then compute  $F(20, 5, F(20, 5, 1))$ , you get an even better approximation, 2.23606 79774 99789 69640 91736 68731 27623 54406 18359 61152 57242 70897 24541 05209 25637 80489 94144 14408 37878 22749 69508 17615 07737 83504 25326 77244 47073 86358 63601 21533 45270 88667 78173  $\dots$ , correct to about 165 places.

## Perfect's Necklace Formula

**Robin Whitty**

The picture below is of a so-called necklace. It has sixteen beads: four black, four grey and eight white. The asterisk is just a label for reference.



By 'necklace' combinatorialists mean a circular permutation of objects belonging to distinguished classes (colours) taking into consideration rotational symmetry. Thus the picture obtained by rotating the beads anti-clockwise until the asterisked white bead reaches the top is still the same necklace. However, if the picture is reflected about a diameter we have a different necklace because the result is not a rotation of the original.

A formula for counting necklaces with a given number of beads and a given number of colours is to be found in many textbooks on combinatorics. Less easy to find is a formula for the case where the number of beads of each colour is fixed. If we have  $t$  colours and there are  $b_1, b_2, \dots, b_t$  beads of each colour, respectively, how many  $(b_1 + \dots + b_t)$ -bead necklaces can we make?

I imagine all combinatorics textbooks give the formula for counting linear  $(b_1 + \dots + b_t)$ -bead arrangements, equivalent to saying that the as-

terisked white bead in our picture is ‘distinguished’. The result is the multinomial coefficient

$$\binom{n!}{b_1, \dots, b_t} = \frac{n!}{b_1! \cdots b_t!},$$

where  $n = b_1 + \dots + b_t$  is the number of beads. In a two-page note in *The Mathematical Gazette* (vol. 40, 1956, pages 45–46), Hazel Perfect uses this solution to find a formula for necklaces.

Perfect’s analysis uses the divisors of the greatest common divisor (gcd) of the bead numbers  $b_i$  to derive a set of linear equations for which she writes down the solution explicitly. My aim is to bypass the linear algebra by using the Möbius function defined on the partial order of divisors. Once you’ve recalled the details I think the resulting formula is simpler to state and more efficient to evaluate.

Perfect’s analysis goes as follows. We have  $n = b_1 + \dots + b_t$  beads. Let  $d$  be the gcd of the  $b_i$ . Then we can find necklaces consisting of  $d$  identical repetitions of bead arrangements of length  $n/d$ . The same is true for any divisor of  $d$ . For the bead numbers in our picture, the greatest common divisor is 4. So there will be necklaces with four repetitions of arrangements of one black, one grey, two white; and necklaces with two repetitions of two black, two grey and four white; and necklaces which are a single four-four-eight arrangement. The necklace in the picture has two repetitions of length 8, starting at the asterisk.

Suppose we call an arrangement consisting of  $k$  identical repetitions a  $k$ -pattern. Every necklace is a  $k$ -pattern for some  $k \geq 1$  dividing the gcd of the  $b_i$ . So if we count  $k$ -patterns for all divisors  $k$  of  $d$  we will have counted all necklaces. Now the number of  $k$ -patterns is just the number of arrangements in any one of its identical repetitions: if we forget about necklaces for a moment and count linear arrangements, then for  $d = \gcd(b_1, \dots, b_t)$  the number of  $d$ -patterns is

$$\binom{n/d}{b_1/d, \dots, b_t/d},$$

and similarly for the divisors of  $d$ .

Summing these multinomials will double count because all linear  $d$ -patterns will also be counted as patterns for any divisor of  $d$ . So we must subtract off these repeat counts. This gives an equation for the number  $p_k$  of linear  $k$ -patterns:

$$p_k = \binom{n/k}{b_1/k, \dots, b_t/k} - \sum_{x \text{ divides } k} p_x. \quad (1)$$

To write an explicitly solvable set of equations for all the linear patterns, write the divisors as a sequence:  $1 = d_1 < d_2 < \dots < d_m = d = \gcd(b_1, \dots, b_t)$ . Let  $S$  be the  $m \times m$  matrix whose  $(i, j)$ -th entry is 1 if  $d_i$  divides  $d_j$  and 0 otherwise. Then extending equation (1) to all patterns and collecting terms:

$$\sum_{j=i}^m S_{ij} p_j = \binom{n/d_j}{b_1/d_j, \dots, b_t/d_j}, \quad i = 1, \dots, m. \quad (2)$$

These equations are solvable since  $S$  is an upper triangular matrix with 1s on the diagonal. Using Cramer's rule we can write down a value for each  $p_i$  as a determinant and summing these values gives the total number of linear arrangements. To count necklaces we need a final observation: a necklace that is a  $k$ -pattern consists of  $k$  repetitions of an  $n/k$ -length arrangement. Cutting the necklace at each point in this arrangement gives  $n/k$  different linear arrangements, and these will be duplicated if we cut anywhere else. If each linear  $k$ -pattern comes from  $n/k$  different necklace  $k$ -patterns, then we should count  $k/n$  necklaces for each  $p_k$ . This completes Hazel Perfect's solution to necklace counting.

Taking the inverse of  $S$  instead of using Cramer, we can write the number of necklaces as:

$$\left(\frac{d_1}{n}, \dots, \frac{d_m}{n}\right) \times S^{-1} \times \left(\binom{n/d_1}{b_1/d_1, \dots, b_t/d_1}, \dots, \binom{n/d_m}{b_1/d_m, \dots, b_t/d_m}\right)^T.$$

The appearance of  $S^{-1}$  is what suggests using the Möbius function, because the  $S$  matrix has entry  $i, j$  equal to 1 precisely if  $i \leq j$  in the partial order of divisors (of  $d$ ). The Möbius function may be defined on the same partial order, as a kind of 'inverse', using the recursive rule:

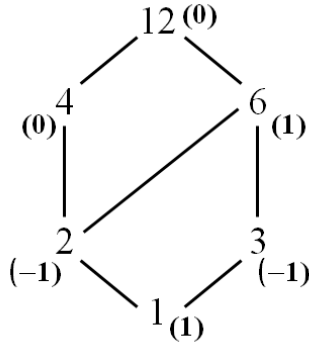
$$\mu(x, y) = \begin{cases} 1 & \text{if } x = y, \\ -\sum_{x \leq z < y} \mu(x, z) & \text{otherwise.} \end{cases}$$

(The first row is just the Möbius function of analytic number theory—restricted to the values in the partial order—which you see in action in M500, issue 206.)

Now the entries of the matrix  $S^{-1}$  are precisely the values of the Möbius function. Here is an example for  $d = 12$ .



	1	2	3	4	6	12
1	1	1	1	1	1	1
2		1	0	1	1	1
3			1	0	1	1
4				1	0	1
6					1	1
12						1
	1	2	3	4	6	12
1	1	-1	-1	0	1	0
2		1	0	-1	-1	1
3			1	0	-1	0
4				1	0	-1
6					1	-1
12						1



Top left: the matrix  $S$  of the partial order of divisors of 12. Right: calculating  $\mu(1, x)$ , for  $x$  in the partial order, starting with  $\mu(1, 1)$  and working upwards. Bottom left: the matrix  $S^{-1}$ . Blank entries are zero.

We can now write down an expression for the number of necklaces with  $b_i$  beads of colour  $i$ ,  $i = 1, \dots, t$  in which linear algebra has been replaced with the arguably simpler and more intuitive Möbius function:

$$\frac{1}{n} \sum_{i=1}^m \sum_{j=i}^m d_i \binom{n/d_j}{n_1/d_j, \dots, n_t/d_j} \mu(d_i, d_j).$$

### Problem 285.2 – Circulant graphs

The *circulant graph*  $Ci(n, S)$  has  $n$  vertices labelled  $0, 1, \dots, n - 1$ , and  $S$  is a subset of  $\{1, 2, \dots, \lfloor n/2 \rfloor\}$ . An edge exists between vertices  $i$  and  $j$  iff  $i - j \equiv s \pmod{n}$  for some  $s \in S$ . For example,  $Ci(n, \{\})$  is the empty graph,  $E_n$ ,  $Ci(n, \{1\})$  is the cycle graph,  $C_n$ , and  $Ci(n, \{1, 2, \dots, \lfloor n/2 \rfloor\})$  is the complete graph,  $K_n$ . The elements of  $S$  are usually called *step sizes*, or just *steps*. There are a few examples on the front cover.

Clearly, the number of possible pairwise non-isomorphic  $Ci(n, S)$  graphs is at most  $2^{\lfloor n/2 \rfloor}$  and, moreover, this limit is actually attained when  $n = 1, 2, 3, 4$ , and  $6$ . Not  $5$  because  $Ci(5, \{1\})$  is isomorphic to  $Ci(5, \{2\})$ .

Prove that there are no other  $n$  for which there exist  $2^{\lfloor n/2 \rfloor}$  pairwise non-isomorphic  $Ci(n, S)$  graphs. Or find another one.

## Solution 282.3 – Array

Which positive integers cannot be represented in the form  $ab+c$ , where  $a$ ,  $b$  and  $c$  are non-negative integers,  $b = a$  or  $b = a - 1$ , and  $c = 0$  or  $c = a - 1$ .

This might have some application. Suppose you wish to arrange  $n$  objects in a square array. If  $n$  is not a square, we must compromise. Perhaps a rectangle with  $a$  rows and  $(a - 1)$  columns will work. And if that can't be done, maybe we can add a column of height  $a - 1$ . Thus  $19 = 4 \times 4 + 3$ , for example.

### Ted Gore

Let  $n$  be a number that can be represented in the manner specified. There are four cases to be considered.

$$\text{Case 1 } (b = a, c = 0): n = a^2 \rightarrow a = \sqrt{n}.$$

$$\text{Case 2 } (b = a - 1, c = a - 1): n = a(a - 1) + (a - 1) \rightarrow a = \sqrt{n + 1}.$$

$$\text{Case 3 } (b = a - 1, c = 0): n = a(a - 1) \rightarrow a = \frac{1 + \sqrt{4n + 1}}{2}.$$

$$\text{Case 4 } (b = a, c = a - 1): n = a^2 + a - 1 \rightarrow a = \frac{-1 + \sqrt{4n + 5}}{2}.$$

It follows that in order to be represented in this way at least one of  $n$ ,  $n + 1$ ,  $4n + 1$ ,  $4n + 5$  must be a perfect square. Any number that does not fit at least one of these conditions cannot be represented. A table of examples is on the next page.

A computer program used the four case definitions to produce a list of all the values up to 225 that cannot be represented as required and a sample of the results follows.

7 10 13 14 17 18 21 22 23 26 27 28 31 32 33 34 37 38 39 40

Note that the results appear in blocks of consecutive numbers with a gap of two missing numbers between blocks.

Let  $X_k$  be the first element of the first block of length  $k$  and let  $Y_k$  be the first element of the second block of length  $k$ . Let  $U_k$  be the last element of the first block of length  $k$  and let  $V_k$  be the last element of the second block of length  $k$ . Then we have:

$$X_k = (k + 1)^2 + (k + 2), \quad U_k = (k + 1)^2 + (2k + 1),$$

$$Y_k = (k + 1)^2 + (2k + 4), \quad V_k = (k + 1)^2 + (3k + 3).$$

Perfect square	$n, a$ for case 1	$n, a$ for case 2	$n, a$ for case 3	$n, a$ for case 4
1	1, 1	0, 1	0, 1	-
4	4, 2	3, 2	-	-
9	9, 3	8, 3	2, 2	1, 1
16	16, 4	15, 4	-	-
25	25, 5	24, 5	6, 3	5, 2
36	36, 6	35, 6	-	-
49	49, 7	48, 7	12, 4	11, 3
64	64, 8	63, 8	-	-
81	81, 9	80, 9	20, 5	19, 4
100	100, 10	99, 10	-	-
121	121, 11	120, 11	30, 6	29, 5
144	144, 12	143, 12	-	-
169	169, 13	168, 13	42, 7	41, 6
196	196, 14	195, 14	-	-
225	225, 15	224, 15	56, 8	55, 7

Now let  $q$  be any positive integer so that  $(k+1)^2$  is the largest perfect square less than or equal to  $q$ . Then  $q$  is representable in the manner given if

$$q = U_k + 1 \quad \text{or} \quad q = U_k + 2 \quad \text{or} \quad q = V_k + 1 \quad \text{or} \quad q = V_k + 2.$$

It is not representable in that manner if  $X_k \leq q \leq U_k$  or  $Y_k \leq q \leq V_k$ . Take 76 as an example. The largest perfect square is 64, so that  $k = 7$ ,  $X_7 = 73$ ,  $U_7 = 79$ , while  $U_7 + 1 = 80$ , which matches case 2 above with  $a = 9$ ,  $b = 8$ ,  $c = 8$ . A little manipulation shows that:

$$U_k + 1 = (k+2)^2 - 1, \text{ which has the form of case 2 when } a = k+2;$$

$$U_k + 2 = (k+2)^2, \text{ which has the form of case 1 when } a = k+2;$$

$$V_k + 1 = (k+2)^2 + (k+1), \text{ which has the form of case 4 when } a = k+2;$$

$$V_k + 2 = (k+3)^2 - (k+3), \text{ which has the form of case 3 when } a = k+3.$$

Also notice that the non-representable numbers can be generated recursively from

$$X_{k+1} = X_k + 2k + 4, \quad Y_k = X_k + k + 2, \quad X_1 = 7.$$

These equations can be used to get a closed equation for  $X_k$  and  $Y_k$ .

I work an example for  $X_4$ .

$$\begin{aligned} X_4 &= X_3 + 2 \cdot 3 + 4 = X_2 + 2 \cdot 2 + 4 + 2 \cdot 3 + 4 \\ &= X_1 + 2 \cdot 1 + 4 + 2 \cdot 2 + 4 + 2 \cdot 3 + 4 = 7 + 2 \sum_{i=1}^3 i + 3 \cdot 4. \end{aligned}$$

Generalizing this we get

$$X_k = 7 + 2 \sum_{i=1}^{k-1} i + 4(k-1) = 7 + k(k-1) + 4(k-1) = k^2 + 3k + 3.$$

And

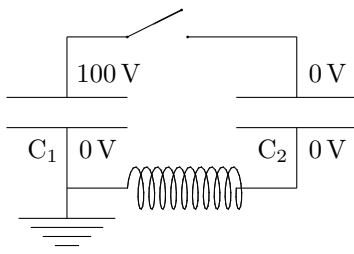
$$Y_k = X_k + k + 2 = k^2 + 4k + 5.$$

The other elements of each block are easily generated from  $X_k$  and  $Y_k$ .

## Problem 285.3 – A coil and two capacitors

### Tony Forbes

This is like Problem 256.5 – Lost energy. Behold, a simple circuit containing a coil of  $L$  henrys and two capacitors of  $C$  farads each. The diagram represents the initial state, with 100 volts across  $C_1$ . Assume the wiring consists of perfect conductors. What happens when you close the switch?



I think the answer lies in the coil. We know from Solution 256.5 that the energy stored in capacitor  $C_1$  is  $100^2 C / 2 = 5000C$  joules. Without the coil half of the energy will be dissipated as heat at infinite amps over zero seconds. After this time each capacitor has 50 volts, hence  $1250C$  joules, and no current flows. I don't know what happens when the coil is added to the circuit. Perhaps I should. I remember doing this kind of stuff at high-school, but that was a long time ago.

## Problem 285.4 – Prime power divisors

Given a number  $d$ , show that every sufficiently large integer has a prime power divisor  $q \geq d$ . For example, if  $d = 6$ , the only integers that fail are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 and 60.

## Solution 254.5 – Descending integers

Find a nice formula as a function of  $n$  for the big number you get by writing down all the  $n$ -digit integers in *descending* order, as in, for example, 999998997...101100 when  $n = 3$ .

### Peter Fletcher

Let  $B_n$  be the number we want ( $B$  for big). Then we have

$$B_3 = 100 + 101\,000 + 102\,000\,000 + \cdots + 999 \text{ [followed by a lot of zeros]}.$$

Thus  $B_n$  can be expressed as a sum and we can also write, for  $n = 3, 4$  and  $5$ ,

$$B_3 = \sum_{k=0}^{899} 1000^k(100 + k), \quad B_4 = \sum_{k=0}^{8999} 10\,000^k(1000 + k),$$

$$B_5 = \sum_{k=0}^{89\,999} 100\,000^k(10\,000 + k).$$

It is clear that for general  $n$ , we can write

$$B_n = \sum_{k=0}^{9 \times 10^{n-1} - 1} 10^{nk}(10^{n-1} + k).$$

I've never come across arithmetico-geometric sequences before, but *Wikipedia* has:

[https://en.wikipedia.org/wiki/Arithmetico\\_geometric\\_sequence](https://en.wikipedia.org/wiki/Arithmetico_geometric_sequence).

There, it gives (replacing their  $n$  with  $m$  for clarity):

$$S_m = \sum_{k=1}^m [a + (k-1)d]r^{k-1} = \left( \frac{a - (a + md)r^m}{1 - r} \right) + \frac{dr}{1 - r} \left( \frac{1 - r^m}{1 - r} \right).$$

Rewriting  $B_n$  as

$$B_n = \sum_{k=1}^{9 \times 10^{n-1}} 10^{n(k-1)}(10^{n-1} + k - 1)$$

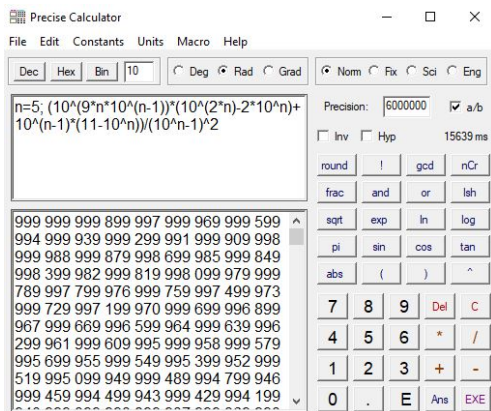
and comparing with *Wikipedia's* expression, we can immediately write down  $m = 9 \times 10^{n-1}$ ,  $a = 10^{n-1}$ ,  $d = 1$  and  $r = 10^n$ . Therefore we can write  $B_n$

as

$$\begin{aligned}
 B_n &= \left( \frac{10^{n-1} - (10^{n-1} + 9 \times 10^{n-1}) \times 10^{9n \times 10^{n-1}}}{1 - 10^n} \right) \\
 &\quad + \frac{10^n}{1 - 10^n} \left( \frac{1 - 10^{9n \times 10^{n-1}}}{1 - 10^n} \right) \\
 &= \frac{1}{(10^n - 1)^2} \left( (10^n - 1)(10^{n-1} + 9 \times 10^{n-1}) \times 10^{9n \times 10^{n-1}} \right. \\
 &\quad \left. - (10^n - 1) \times 10^{n-1} + 10^n - 10^{9n \times 10^{n-1} + n} \right) \\
 &= \frac{10^{9n \times 10^{n-1}} (10^{2n} - 2 \times 10^n) + 10^{n-1} (11 - 10^n)}{(10^n - 1)^2}.
 \end{aligned}$$

I checked this in MAPLE for  $n = 1$ ,  $n = 2$  and  $n = 3$ , and it works. With  $n = 4$  and  $n = 5$  MAPLE can't show the full number, just the first and last 100 digits, but it certainly appears to work with these numbers as well.

**TF** — PRECCALC64 also has no trouble verifying the final formula, above, exactly for  $B_4$  and  $B_5$ . The screen-shot on the right shows in the top window how to set up the calculation, and you can clearly see the first part of the result,  $B_5$ , which appears in the bottom window after 15.639 seconds. There is a scroll-bar to let you see the rest of the number.



## Problem 285.5 – 64 cubes

This is very similar to Problem 274.5 – 27 cubes. There are 64 cubes, where each face is painted using one of the four colours red, blue, green, yellow (or, if you prefer, light grey, medium grey, dark grey, black). Moreover, the 64 cubes can be assembled in four ways to form either a red, blue, green or yellow  $4 \times 4 \times 4$  cube. How can this be achieved?

What about  $n^3$  cubes,  $n$  colours and  $n$  monochromatic  $n \times n \times n$  cubes?

---

## Observations regarding ‘Bedlam Cube’ solution by computer

**Chris Pile**

I was very pleased to see the collection of pentacubes on the cover of issue M500 **282**, and the article on the ‘Bedlam Cube’ by Rob Evans, who kindly mentioned my articles in M500 **134** and **152**. I purchased the puzzle more than 25 years ago from an elderly lady at a car boot sale, with the box and pieces loose in a polythene bag; so I did not have the opportunity of seeing it completed or taking it apart slowly! It was four years later that by a stroke of good fortune I was finally able to put all 13 pieces into the box! My computer would have taken aeons, but was able to confirm the solution, given a head start of six pieces located correctly, in just a few minutes.

Having written a program that would (eventually!) have solved the puzzle I do not have the same enthusiasm for revisiting the task. However, with the benefit of hindsight I could have reduced the number of combinations. My program fitted each piece in turn in a predetermined order, as described by Rob Evans, starting with the ‘+’ piece, which, as stated, has only two places (ignoring symmetrical positions) within the  $4 \times 4 \times 4$  box. This piece is also the only piece which cannot be fitted into a vertex of the box. The tetra-cube is the only piece which need not have a face showing on the  $4 \times 4 \times 4$  cube.

The selection of each piece should, as Rob explains, be made wisely to reduce the number of combinations. He considers ‘neighbours’ with a face in common. My instinct would be to consider which pieces could have a vertex, edge or face with the  $4 \times 4 \times 4$  box in common. Eight of the twelve pieces must fit into a vertex. If each piece was coloured to show whether a face could appear in a vertex, edge or face of the box, it might facilitate a manual solution. The computer program should check whether an impossible void is created after each piece is placed.

The label on the box claims that there are hundreds of correct solutions. My program found two solutions (with a little help!) in about 20 minutes (only small differences in solutions).

As I mentioned M500 **152**, I was able to put 25 pentacubes (excluding the four pieces with dimension at least 4 cubes) into a  $5 \times 5 \times 5$  cube. If I used these four pieces, it was very easy to make up a  $5 \times 5 \times 5$  cube with four other pieces remaining. I found other solutions quite easily. I enjoy the challenge of doing this type of puzzle manually and therefore I wait for someone else to check all 23751 cases!

---

## Magic numbers

### Sebastian Hayes

**Definition** A number  $N$  is *magic* if any number which ends with  $N$  is divisible by  $N$ . Base 10 is assumed.

**Example** Any number ending in 2 is even and thus divisible by 2.

**Problem** (a) How many magic numbers are there less than or equal to  $10^n$ ? (b) Give a sufficient and necessary condition for a number (positive integer) to be magic.

**Solution** The key point to grasp is that if a number  $N$  is to divide any number which ends  $\dots N$ , it must divide the first power of 10 greater than  $N$ . For if it does this, it will divide any multiple of this power, and this covers all numbers with more digits than  $N$  which terminate with  $\dots abcd = N$ .

By trial we find that 1, 2 and 5 are the only magic numbers less than 10. And, excluding these, below 100 we have 10, 20, 25 and 50. For  $n \geq 2$ , there seem to be five magic numbers with  $n$  digits between  $10^n$  and  $10^{n+1}$ , where we include the lower limit  $10^n$  but not the higher. For example, if we consider magic numbers with four digits we are looking for numbers which divide  $10^4$  and are at least  $10^3$ . Now, the only factors of powers of 10 are powers of 2 and 5; so the only possibilities are  $10^4/2 = 5000$ ,  $10^4/4 = 2500$ ,  $10^4/5 = 2000$ ,  $10^4/8 = 1250$  and  $10^4/10 = 1000$ . Any other numbers which divide  $10^4$  will have fewer than four digits.

More generally, for  $n \geq 2$  over  $[10^{n-1}, 10^n)$ , we have the five numbers:  $10^n/2^1$ ,  $10^n/2^2$ ,  $10^n/5$ ,  $10^n/2^3$  and  $10^{n-1}$ , or

$$5^{n-1}2^n, \quad 5^n2^{n-1}, \quad 5^n2^{n-2}, \quad 5^n2^{n-3}, \quad 5^{n-1}2^{n-1}.$$

(For  $n = 1$ ,  $n = 2$ , we get fewer because we have to discount fractional divisors such as  $10^2/2^3$  or  $10^1/2^3$ .)

Since there are three magic numbers between 1 and 10, four between 10 and 100 (including 1 and 10), and five in all subsequent stretches between  $10^{n-1}$  and  $10^n$  the answer to the first part of the problem is  $5(n-2) + 7$ , and if we include  $10^n$  itself, we obtain the result.

There are  $5n - 2$  magic numbers between 1 and  $10^n$  inclusive,  $n \geq 2$ .

Bearing the above in mind, it will be seen that the following is a necessary and sufficient condition:

$$N \text{ is magic if } N = 2^p5^q, \text{ where } 0 \leq q - p + 1 \leq 4.$$

I came across this problem in *The Mathematical Experience* by Philip J. Davis and Reuben Hersh.



## Japanese clock

### Ralph Hancock

Until the end of the Tokugawa shogunate in 1868, Japan used a traditional timekeeping system in which the length of the hours varied according to the length of the day. Using modern numbering for the hours, sunrise was always at 06:00 and sunset always at 18:00, summer or winter. Therefore the length of hours varied.

The Japanese devised a clock with variable hours, known as a *wadokei*. They used various methods of adapting a clock running at a fixed rate to show the correct hour, such as a set of replaceable dials, or dials in which the markers could be slid around. In these, the clock had to be manually reset at frequent intervals.

Some of these clocks, using different methods, can be seen at

<http://www.jcwa.or.jp/en/etc/wadokei.html>.

Usually the dial revolved rather than the hour hand.

It seems that it might be possible to make a mechanical clock with a conventional moving hour hand and an elliptical dial that is automatically slid up and down over the course of a year so that the hour hand is always approximately right – ‘approximately’ because the rotation of the earth is a bit wobbly. Here are the data for sunrise and sunset times in Tokyo (which, as the principal city in the Tokugawa era, was called Edo) in 2018. As you will see, here modern clock time is about 20 minutes earlier than local sun time. Tokyo is at  $35^{\circ}41'22''\text{N}$   $139^{\circ}41'30''\text{E}$ .

At the spring equinox, 21 March in 2018, sunrise is at 05:44 and sunset is at 17:53.

At the summer solstice, 21 June in 2018, sunrise is at 04:25 and sunset is at 19:00.

At the autumn equinox, 23 September in 2018, sunrise is at 05:29 and sunset is at 17:37.

At the winter solstice, 22 December in 2018, sunrise is at 06:47 and sunset is at 16:31.

Can you design a clock dial that moves up and down as required and whose hour hand shows local sun time accurately to the nearest 10 minutes according to the traditional convention?

---

## Solution 276.1 – Three dice

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

### Dave Wild

Assume the largest number is  $N$ . If at least one of the other dice shows the same number then either all three dice show the number  $N$  or, if possible, two of them show the number  $N$  and the other one a number less than  $N$ . There are  $1 + 3(N - 1) = 3N - 2$  ways this can occur.

The total number of ways the maximum number on the three dice can be  $N$  can be calculated by calculating the number of ways the values on the three dice are each  $N$  or less, and then subtracting the number of times the numbers on the three dice are, if possible, less than  $N$ . This gives  $N^3 - (N - 1)^3$  possibilities.

The table below shows the probability that at least two of the dice have the largest number revealed by the host.

Largest number	1	2	3	4	5	6
	1/1	4/7	7/19	10/37	13/61	16/91
	100%	57%	37%	27%	21%	18%

Before the host shows you the largest number the probability of at least two dice showing the largest number is

$$\frac{1 + 4 + 7 + 10 + 13 + 16}{216} = \frac{17}{72},$$

or approximately 24%.

**Words** Find the correct one-word answers to the following clues. What have they in common? Solution in a future issue.

(1) A colour (2) Went higher (3) Neat lines of things (4) A girl's name (5) Eggs from many fish (6) Got out of bed (7) Belongs to a girl (8) Propels a small boat (9) Belongs to a Greek letter (10) Belongs to the eggs of a fish (11) A flower (12) Many girls with the same name (13) Watering can nozzle (14) Belongs to a horizontal line of a table (15) Belongs to a small deer (16) Many Greek letters (17) Many small deer (18) Unspecified belligerent in 15th century civil war (19) Ceiling light fitting (20) Decorative compass card (21) Shower outlet (22) Belongs to the eggs of many fish (23) Belongs to many small deer (24) Belongs to all the horizontal sections of a matrix (25) Garden never promised in song

---

## M500 Mathematics Revision Weekend 2019

The forty-fifth M500 Revision Weekend will be held at

**Kents Hill Park Training and Conference Centre,**

**Milton Keynes, MK7 6BZ**

**from Friday 10th to Sunday 12th May 2019.**

The standard cost, including accommodation (with en suite facilities) and all meals from dinner on Friday evening to lunch on Sunday is £275 for single occupancy, or £240 per person for two students sharing in either a double or twin bedded room. The standard cost for non-residents, including Saturday and Sunday lunch, is £160.

Members may make a reservation with a £25 deposit, with the balance payable at the end of February. Non-members must pay in full at the time of application and all applications received after 28th February 2019 must be paid in full before the booking is confirmed. Members will be entitled to a discount of £15 for all applications received before 10th April 2019. The Late Booking Fee for applications received after 10th April 2019 is £20, with no membership discount applicable.

There is free on-site parking for those travelling by private transport. For full details and an application form, see the Society's web site:

[www.m500.org.uk](http://www.m500.org.uk).

The Weekend is open to all Open University students, and is designed to help with revision and exam preparation. We expect to offer tutorials for most undergraduate and postgraduate mathematics OU modules, subject to the availability of tutors and sufficient applications.

---

*Please note that the venue is not the same as last year.* It can be very confusing; so we will state the address a couple more times to make sure we have got it right.

Kents Hill Park Training and Conference Centre, Milton Keynes

Kents Hill Park Training and Conference Centre, Milton Keynes

---

### M500 Society membership year change

To align with OUSA, and other OU societies, the M500 Society financial year, and consequently membership year, will change to 1 August – 31 July. To accommodate the transition, 2018 membership will be extended to 31 July 2019.

**Ramblings round representations – Part 2**

Roger Thompson ..... 1

**Problem 285.1 – Roots**..... 11

**Perfect’s Necklace Formula**

Robin Whitty ..... 12

**Problem 285.2 – Circulant graphs** ..... 15

**Solution 282.3 – Array**

Ted Gore ..... 16

**Problem 285.3 – A coil and two capacitors**

Tony Forbes ..... 18

**Problem 285.4 – Prime power divisors** ..... 18

**Solution 254.5 – Descending integers**

Peter Fletcher ..... 19

**Problem 285.5 – 64 cubes**..... 20

**Observations regarding ‘Bedlam Cube’ solution by computer**

Chris Pile ..... 21

**Magic numbers**

Sebastian Hayes ..... 22

**Japanese clock**

Ralph Hancock ..... 23

**Solution 276.1 – Three dice**

Dave Wild ..... 24

**M500 Mathematics Revision Weekend 2019** ..... 25

**Problem 285.6 – Two integrals**..... 26

04.00

**Problem 285.6 – Two integrals**

Show that

$$\int_0^1 \left( \frac{\cos(1/x)}{x} + (\sin x)(\log x) \right) dx = -\gamma$$

and that

$$\int_0^1 \left( 2x \cos \frac{1}{x} - (\sin x)(\log x) \right) dx = \gamma + \cos 1 - \sin 1.$$

Recall that  $\gamma = \lim_{n \rightarrow \infty} \left( \sum_{k=1}^n \frac{1}{k} - \log n \right) = \int_1^{\infty} \left( \frac{1}{[x]} - \frac{1}{x} \right) dx = 0.57721566\dots$