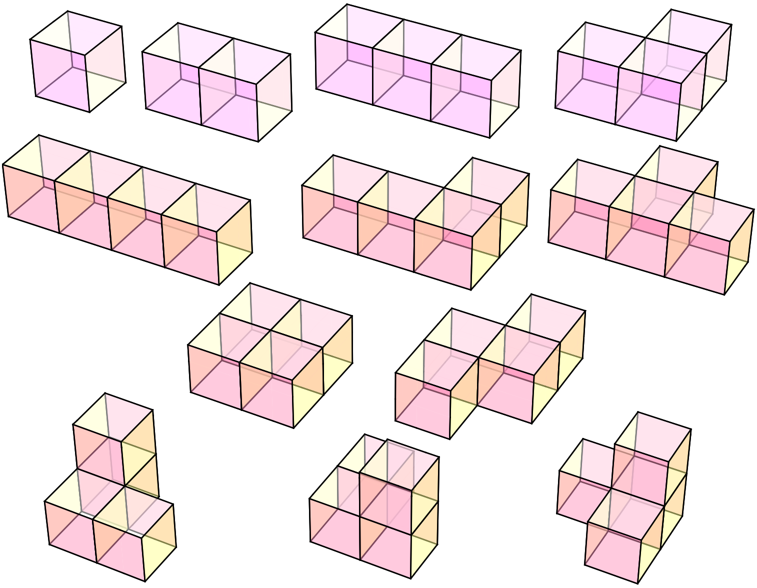
*

ISSN 1350-8539

M500 284



The M500 Society and Officers

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

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

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

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

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/` from where a LaTeX template may be downloaded.

M500 Mathematics Revision Weekend 2019

The M500 Revision Weekend 2019 will be held at

Kents Hill Park Training and Conference Centre, Milton Keynes
MK7 6BZ
from Friday 10th to Sunday 12th May 2019.

We expect to offer tutorials for most undergraduate and postgraduate mathematics Open University modules, subject to the availability of tutors and sufficient applications. Application forms will be sent via email to all members who included an email address with their membership application or renewal form. Contact the Revision Weekend Organizer, **Judith Furner**, at weekend@m500.org.uk if you have any queries about this event.

Ian Harrison

With sadness we have to report to you the death of a much loved supporter and friend of M500.

Ian Harrison was a member of the mathematics staff of the Open University for many years. He retired in 2005, and that left him free to enjoy full-time his passionate interest in origami and geometry. He was a long-term, active member of the British Origami Society.

Of course, many of you will know Ian as the dynamic presenter of our M500 Winter Weekend. Every January from 1993 to 2006 Ian would delight us at Florence Boot Hall, with his lively programmes of mathematical entertainments, lectures and group problem-solving activities. And he was not one to shy away from tackling challenging material. His sessions at the Winter Weekend were an inspiration to us all and one never left without one's head spinning with all kinds of interesting ideas.

Ian was an M500 Revision Weekend tutor for M203 back in the days of big student numbers, and if you were involved with that course, you would probably remember him as director of the summer school.

Ian died on Thursday 30th August 2018 after a battling with cancer for two and a half years. We offer our sympathy to his family, especially son Mark, daughter Dawn and brother Chris. Rest in peace, Ian.

Ramblings round representations – Part 1

Roger Thompson

1 Introduction

In the article 'Factorization using the Number Field Sieve' in M500 **275**, I introduced prime representations in the context of monic irreducible cubic polynomials. This series of three articles[1] explores this subject further, using it to attempt to show how some of the concepts of algebraic number theory arise naturally, but without assuming any prior knowledge. Inevitably, some aspects have to be taken on trust. Conrad (2003) alludes to the subject, but I have found very little else in the literature, so the empirical results presented here must be regarded as highly speculative. I would welcome any theoretical insights from readers on any such results.

Unless otherwise stated, all polynomials in these articles have integer coefficients. We will need the notation and some results from M500 **275**. To recap briefly:

[1] Parts 2 and 3 and will appear in issues **285** and **286** respectively

> We use mod f to indicate the remainder when some polynomial is divided by f. This is equivalent to evaluating polynomials with x set to one of the roots of $f(x) = 0$. We will use X to indicate one of those roots, but also more importantly to allow polynomials to be treated as algebraic entities.
>
> We use mod f, p to indicate that algebra is conducted mod f, but that all coefficients are calculated mod p.

Let

$$g \;=\; aX^2 + bX + c, \quad f \;=\; X^3 + PX^2 + QX + R.$$

Then if $f(X) = (X - \alpha)(X - \beta)(X - \gamma)$, where α, β, γ are the roots of f, we define the norm $N(g) = g(\alpha)g(\beta)g(\gamma)$. This is an integer, and is the determinant of the matrix

$$A(g, f) \;=\; \begin{pmatrix} c & -aR & (aP - b)R \\ b & c - aQ & (aP - b)Q - aR \\ a & b - aP & (aP - b)P - aQ + c \end{pmatrix}.$$

Expressions with norm ±1 are called units. Using the above definition, the norm of an arithmetic prime number p is p^3. We might therefore suspect that if a prime p has an integer root for $f \equiv 0 \bmod p$, then p has factors mod f. We will call a polynomial g such that $g(r) \equiv 0 \bmod p$ and $N(g) = p$ a **representation** of p_r, denoting g by $\rho(p_r)$.

We will need an additional definition. The **discriminant** Δ of f is defined as $[(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)]^2$, and can be calculated directly from the coefficients:

$$\Delta \;=\; P^2Q^2 - 4Q^3 - 4P^3R - 27R^2 + 18PQR.$$

If $\Delta < 0$, then f has a single real root. The rest of this article confines itself to such f.

2 Coefficients of representations

The determinant $A(g, f)$ has the distinctly unpromising expression

$$\begin{aligned} &R^2a^3 - Rb^3 + c^3 - QRa^2b + PRab^2 + (Q^2 - 2PR)a^2c \\ &\quad + (P^2 - 2Q)ac^2 + Qb^2c - Pbc^2 + (3R - PQ)abc. \end{aligned}$$

However, we can put it to good use quite simply. Let $g(X) = X^2 + \mu X + \nu$ for some reals μ, ν. We investigate values of μ, ν such that $g^2 \equiv \kappa g \bmod f$ for some real κ.

Since norms are completely multiplicative, we have $N(g)^2 = N(\kappa)N(g)$. If $N(g) \neq 0$, then $N(\kappa) = \kappa^3 = N(g)$, which doesn't help. However, if $N(g) = 0$, we can calculate the values of μ and ν by working out $g^2 \bmod f$

explicitly. We get

$$\begin{aligned}\kappa &= \mu^2 + 2\nu - Q - 2\mu P + P^2,\\ \kappa\mu &= 2\mu\nu - R - 2\mu Q + PQ,\\ \kappa\nu &= \nu^2 - 2\mu R + PR.\end{aligned}$$

So

$$\mu^3 - 2P\mu^2 + (P^2 + Q)\mu + R - PQ \;=\; \nu^2 + B\nu + C \;=\; 0,$$

where $B = (\mu - P)^2 - Q$ and $C = (2\mu - P)R$. Note that $\mu = P + \alpha$, where α is the real root of f. Empirically, we choose $\nu = \dfrac{-B + \sqrt{B^2 - 4C}}{2}$.

We might expect that by approximating μ and ν by rationals b/a and c/a, we get $N(aX^2 + bX + c) = 1$, yielding a unit, or $N(aX^2 + bX + c) = p$ for some prime p for which $f(r) \equiv 0 \bmod p$ for some integer r, yielding the representation $\rho(p_r)$. This expectation is amply borne out in practice.

A given unit U with $N(U) = 1$ may be the power greater than 1 of some other unit, which is in some sense more fundamental. We can check if this is the case by evaluating $x = U^{1/p}(\alpha)$ for successive primes p, where α is the real root of f, and using an integer relation finding algorithm such as PSLQ to attempt to find integers A, B, C such that $A\alpha^2 + B\alpha + C = x$. We do this repeatedly until no further reduction can be done. We are left with a unit U_1 and another U_2 such that $U_1U_2 \equiv 1 \bmod f$. For any quadratic $q = aX^2 + bX + c$, the Euclidean norm is $\|q\| = \sqrt{(a^2 + b^2 + c^2)}$. We will need to apply this to norms N; so to avoid confusion, we will call $\|q\|$ the **magnitude** of q.

By convention, we will label the unit $aX^2 + bX + c$ for which b/a, c/a are most closely approximated by μ, ν as U_1. More precisely, if $a_nX^2 + b_nX + c_n \equiv U_1^n \bmod f$, then $b_n/a_n \to \mu$, $c_n/a_n \to \nu$ as $n \to \infty$. When writing out $\rho(p_r)$, we choose the form such that $\|\rho(p_r)U_k^n\|$ is minimized (k = 1 or 2).

If $\rho(p_r)$ exists for every p_r, then there will be some minimum a such that

$$N(aX^2 + \mathrm{nint}(\mu a)X + \mathrm{nint}(\nu a)) \equiv \rho(p_r)U_k^n \bmod f,$$

where $\mathrm{nint}(x)$ is the nearest integer to x. In other words, the p_r can be ordered by their a value as well as their numerical value. Example for $X^3 + X^2 + 2X + 1$ with $U_1 = X^2 + 1$, $U_2 = X^2 + X + 1$.

Let

$$D \;=\; \frac{\text{Numerical order ordinal } \rho(p_r)}{a \text{ order ordinal } \rho(p_r)U_k^n}.$$

Empirically, for a large number of $\rho(p_r)$, $\log(D)$ has upper and lower bounds, with each tending to a limit. It might be better to use a weighted form of

Euclidean norm for magnitudes, e.g. $\sqrt{a^2 + (b^2/\mu^2) + (c^2/\nu^2)}$, but we only really need a qualitative measure. If $\|U_1\|$ or $\|U_2\|$ is large, we might expect that some $\|\rho(p_r)\|$ are large even for small p. This is exactly what we see. For example, if $f = X^3 + X^2 + 61X + 300$, then

$$\mu \;=\; -\,3.07853145152515, \quad \nu \;=\; 73.5558873495547$$

with

$$\begin{aligned} U_1 &= 410322478704071121356496552X^2 \\ &\qquad -\,126319065595824256988446792 8X \\ &\qquad +\,30181634020546719076316795761, \\ U_2 &= -\,1996276307688X^2 + 6184172650392X + 58429238801041. \end{aligned}$$

We have $\rho(4759_{1185}) = 4X + 19$ and yet

$$\rho(4759_{2574}) \;=\; 93362148X^2 - 287418309X + 6867335641.$$

Ordinal	Numerical order	a order
1	$\rho(5_1) : -X + 1$	$U_1^7\rho(5_1) : 6X^2 + 3X + 11$
2	$\rho(7_5) : X^2 - X + 1$	$U_1^9\rho(7_5) : 13X^2 + 6X + 23$
3	$\rho(11_7) : -X^2 + 2X + 2$	$U_1^{14}\rho(11_7) : 15X^2 + 6X + 26$
4	$\rho(17_2) : -X + 2$	$U_1^{14}\rho(23_5) : 27X^2 + 12X + 47$
5	$\rho(19_{10}) : -2X + 1$	$U_1^{10}\rho(23_{20}) : 29X^2 + 12X + 51$
6	$\rho(23_5) : -X^2 - 4X - 1$	$U_1^{11}\rho(17_2) : 31X^2 + 13X + 54$
7	$\rho(23_{20}) : 2X^2 - X + 2$	$U_1^{12}\rho(19_{10}) : 34X^2 + 15X + 60$
8	$\rho(37_7) : -2x^2 + 3X + 3$	$U_1^{11}\rho(43_3) : 43X^2 + 18X + 75$
9	$\rho(43_3) : -X + 3$	$U_1^{18}\rho(37_7) : 55X^2 + 24X + 97$
10	$\rho(53_6) : -3X^2 - 8X - 3$	$U_1^{13}\rho(59_{10}) : 59X^2 + 25X + 104$
11	$\rho(59_{10}) : -X^2 - 2X + 2$	$U_1^{23}\rho(59_{37}) : 71X^2 + 31X + 125$
12	$\rho(59_{11}) : -X^2 - 5X - 1$	$U_1^{14}\rho(61_{19}) : 85X^2 + 37X + 149$
13	$\rho(59_{37}) : -6X^2 + 5X + 5$	$U_1^{14}\rho(101_{76}) : 92X^2 + 40X + 161$
14	$\rho(61_{19}) : X^2 - 3X + 1$	$U_1^{17}\rho(59_{11}) : 99X^2 + 43X + 174$
15	$\rho(67_{41}) : 2X^2 - 2X + 3$	$U_1^{13}\rho(67_{41}) : 101X^2 + 43X + 177$

3 The arithmetic of norms

By definition, $\rho(p_r)(r) \equiv 0 \bmod p$; so $[g\rho(p_r)](r) \equiv 0 \bmod f, p$ for any polynomial g. For a particular prime p, $f(r) \equiv 0 \bmod p$ has zero, one or three roots (counting repeated roots as distinct). To illustrate what these two statements imply, we will use

$$f \;=\; X^3 + X^2 + 17X + 12.$$

From now on, we will use f to represent appropriate polynomials in general, and ξ to represent our example polynomial. For $p = 173$, there are three roots 62, 115, 168, and each has a representation:

$$\rho(173_{62}) = 2X^2 + X + 35, \quad \rho(173_{115}) = -3X - 1, \quad \rho(173_{168}) = X + 5.$$

We will see how to find representations in Part 3. Setting

$$g \;=\; \rho(173_{62})\rho(173_{115}),$$

we have

$$[\rho(173_{62})\rho(173_{115})\rho(173_{168})](r) \;\equiv 0 \mod \xi, p$$

for $r = 62$, 115, 168, and

$$N(\rho(173_{62})\rho(173_{115})\rho(173_{168}) \bmod \xi) \;=\; 173^3 \;=\; N(173);$$

so

$$\rho(173_{62})\rho(173_{115})\rho(173_{168}) \;\equiv\; 173 \bmod \xi.$$

This is true in general for any f with three roots r, s, t mod p, i.e.

$$\rho(p_r)\rho(p_s p_t) \;\equiv\; \rho(p_r)\rho(p_s)\rho(p_t) \;\equiv\; p \bmod f.$$

There is another polynomial $\tau(p_r)$ such that $\rho(p_r)\tau(p_r) \equiv (X - r) \bmod f$. Evaluating $N(X - r)$ from the formula in the previous section, we find $N(X - r) = -f(r) = -kp$ for some k; so $N(\tau(p_r)) = -k$. In our example,

$$\begin{aligned}\tau(173_{62}) \;&=\; X^2 + 6X + 2, \quad \tau(173_{115}) \;=\; -6X^2 - 4X - 101,\\ \tau(173_{168}) \;&=\; -X^2 + 4X - 36.\end{aligned}$$

By definition, $(X - r)Y \equiv f \bmod p$ for some quadratic Y with $Y = (X - s)(X - t)$ in the three root case. We can extend the above results to the case where $f(r) \equiv 0 \bmod p$ only has one root. For ξ, $p = 239$ has the single root 45; so dividing $X - 45$ into ξ, we get $Y = X^2 + 46X + 175$. We find

$$\rho(239_{45}) \;=\; -X^2 - 8X - 5,$$

and that

$$\rho(239_{45})(68X^2 + 21X + 1145) \;\equiv\; 239 \bmod \xi,$$

with both sides $\equiv 0 \mod \xi, p$ as required, and $N(68X^2 + 21X + 1145) = 239^2$. We will write

$$\rho(239^2_*) \;=\; 68X^2 + 21X + 1145$$

to signify that this representation is not tied to any root. This is also true in general for any f with a single root r mod p, i.e. $\rho(p_r)\rho(p^2_*) \equiv p \bmod f$. Similarly, we have $\rho(239^2_*)\tau(239^2_*) \equiv Y \bmod \xi$, where $\tau(239^2_*) = -2X^2 - 3X - 1$.

To avoid having different notations for the single and three roots cases where the distinction does not matter, we will say $\rho(p_r)\sigma(p_r) \equiv p \bmod f$, where $\sigma(p_r) = \rho(p_*^2)$ and $\sigma(p_r) = \rho(p_s)\rho(p_t)$ respectively. Similarly, we will say $\rho(p_r)\upsilon(p_r) \equiv (X - r)Y \bmod f$, where $\upsilon(p_r) = \tau(p_*^2)$ and $\upsilon(p_r) = \tau(p_s)\tau(p_t)$ respectively. With much tedious algebra, it can be shown that σ, τ and υ have integer coefficients. If $f(r) \equiv 0 \bmod p$ has no roots, then there is only a representation for p^3, i.e. p itself.

In the next section, we have a look at cases where roots exist but representations do not. This will reveal the origins of algebraic number theory, founded in the 19th century by Kummer and Dedekind. This will necessarily be a very informal introduction, but may nevertheless provide some insight into how the concept of ideals arises naturally.

4 Unique factorization lost and regained

We will continue to use our example polynomial $\xi = X^3 + X^2 + 17X + 12$. Note that $\xi \equiv 0 \bmod 3$ has a single root 0, with $X(X^2+X+2) \equiv \xi \bmod 3$, and $\xi \equiv 0 \bmod 61$ has three roots, with $(X-6)(X-16)(X-38) \equiv \xi \bmod 61$. However, none of $\rho(3_0)$, $\rho(61_6)$, $\rho(61_{16})$, $\rho(61_{38})$, exist. Define

$$g \;=\; 104X^2 + 30X + 1749, \quad h \;=\; 5X^2 + 2X + 85.$$

We find that $gh \equiv 183U_1 \bmod \xi$, where $U_1 = 49X^2 + 14X + 823$ is a unit. Also $N(g) = 61^2 3$, $N(h) = 3^2 61$, $N(183) = 3^3 61^3$. Now $g(0) \equiv 0 \bmod 3$, $g(6), g(16) \equiv 0 \bmod 61$, $g(38) \not\equiv 0 \bmod 61$, $h(0) \not\equiv 0 \bmod 3$, $h(38) \equiv 0 \bmod 61$, $h(6), h(16) \not\equiv 0 \bmod 61$. In other words, g could be thought of as $\rho(3_0 61_6 61_{16})$, and h as $\rho(3_*^2 61_{38})$. As we already saw, multiplication accumulates roots mod p; so that in this case, $gh(r) \equiv 0 \bmod \xi, p$ for all roots r of 3 and 61, hence

$$gh \;=\; (104X^2 + 30X + 1749)(5X^2 + 2X + 85) \;\equiv\; 3 \times 61 \bmod \xi.$$

Given that g and h are irreducible, and 3 and 61 are primes, we have two distinct factorizations mod ξ.

In the familiar world of integers, the Fundamental Theorem of Arithmetic proves that any integer can be factorized into a product of prime factors in essentially a unique way, i.e. ignoring reordering of the factors. When working modulo f, we also have to ignore multiples of units. However, we have just seen that even taking this into account still leaves us with non-unique factorization in some cases.

However, we have also seen that where representations exist, primes can be split and recombined in different ways. For example, consider

$$(10X^2 - 213X - 149)(-72X^2 + 34X + 67) \;\equiv\; 173 \times 239(-7X - 5) \bmod \xi.$$

Clearly, $N(-7X - 5) = 1$; so $-7X - 5$ is a unit, and we appear to have another example of non-unique factorization. However, we find that

$$10X^2 - 213X - 149 \;\equiv\; \rho(173_{62})\rho(173_{115})\rho(239_{45}) \bmod \xi,$$

and

$$-72X^2 + 34X + 67 \;\equiv\; \rho(173_{168})\rho(239)_*^2(-7X-5) \bmod \xi.$$

Rearranging factors, we see that the product is

$$\begin{aligned}&\rho(173_{62})\rho(173_{115})\rho(173_{168})\rho(239_{45})\rho(239)_*^2(-7X-5)\\ &\qquad\qquad\equiv\; 173 \times 239(-7X-5) \bmod \xi;\end{aligned}$$

so the factorizations are not distinct after all. We would like to make non-unique factorization go away by being able to rearrange factors similarly, even though the associated representations do not exist.

In the three root case, we consider all polynomials $q \bmod f$ for which $q(r) \equiv 0 \bmod p$, where r is such that $f(r) \equiv 0 \bmod p$. Since $f(X) = 0$, q must be of the form $q_1(X-r) + q_2 p \bmod f$ for arbitrary polynomials q_1, q_2 of degree at most 2. We write $\langle X-r, p\rangle$ to mean the set of polynomials generated by $X-r$, p in this way, and refer to $\langle X-r, p\rangle$ as an **ideal**. Now

$$q_1(X-r) + q_2 p \;\equiv\; q_3\rho(p_r) \bmod f, \;\text{ where }\; q_3 \;=\; q_1\tau(p_r) + q_2\sigma(p_r);$$

so $\langle X-r, p\rangle = \langle\rho(p_r)\rangle$. An ideal that has a single generator is called a **principal ideal**; so p_r has a representation if and only if $\langle X-r, p\rangle$ is principal, in which case it has the generator $\rho(p_r)$. We next consider how to multiply ideals.

Since $\langle a\rangle$ is the set of polynomials $\{aq_1 \bmod f\}$ for any polynomial q_1, it follows that $\langle a\rangle\langle b\rangle$ is the set of polynomials

$$\{q_1 q_2 ab \bmod f\} \;=\; \{q_3 ab \bmod f\}$$

for any polynomial q_3. As an example of multiplying non-principal ideals, we consider $X^2+15 \bmod \xi$, which has norm 69; $\xi \bmod 3$ has the single root 0, and $\xi \bmod 23$ has the single root 13, but there are no representations for $3_0, 23_{13}$:

$$\begin{aligned}\langle X^2+15\rangle \;&=\; \{(aX^2+bX+c)(X^2+15) \bmod \xi\}\\ =\; \{(c-a-b)X^2 + (5a-2b)X + 15c - 12b + 12a\} \;&=\; \{uX^2+vX+w\},\end{aligned}$$

where

$$a = \frac{-30u+3v+2w}{69},\; b = \frac{-75u-27v+5w}{69},\; c = \frac{-36u-24v+7w}{69}.$$

In other words, we have to show that for any uX^2+vX+w in the set of polynomials generated by $\langle X, 3\rangle\langle X-13, 23\rangle$,

$$-30u+3v+2w,\;\; -75u-27v+5w \;\text{ and }\; -36u-24v+7w$$

are all divisible by 69. It is no coincidence that 69 is the norm of $X^2 + 15$. The reader may like to work out why. Now

$$\begin{aligned}\langle X, 3\rangle\langle X-13, 23\rangle &= \{(Xq_1 + 3q_2)((X-13)q_3 + 23q_4) \bmod \xi\}\\ = X(X-13)q_1q_3 + 69q_2q_4 + 3(X-13)q_2q_3 + 23Xq_1q_4 &= A+B+C+D,\end{aligned}$$

say. Clearly, B is always divisible by 69. Moreover,

$$\begin{aligned}C &= 3(X-13)(aX^2+bX+c)\\ &\equiv 3(b-14a)X^2 + 3(c-13b-17a)X - 3(13c+12a) \bmod \xi\\ &= uX^2+vX+w,\end{aligned}$$

say. Furthermore,

$$\begin{aligned}-30u + 3v + 2w &= 69(15a - 3b - c),\\ -75u - 27v + 5w &= 69(63a + 12b - 4c),\\ -36u - 24v + 7w &= 69(36a + 12b - 5c);\end{aligned}$$

so C is always divisible by 69. Since this means $(X-13)(aX^2+bX+c)$ is always divisible by 23, A and D are always divisible by 23. Now

$$X(aX^2+bX+c) \equiv (b-a)X^2 + (c-17a) - 12a \bmod \xi;$$

so substituting as before, we see A and D are always divisible by 3, and hence by 69. We have therefore shown $\langle X, 3\rangle\langle X-13, 23\rangle = \langle X^2+15\rangle$.

We have already seen that $\rho(173_{62})\rho(173_{115})\rho(173_{168}) \equiv 173 \bmod \xi$. When all three representations exist, we can write factorizations as before in terms of ideals. For example,

$$\langle\rho(173_{62})\rangle\langle\rho(173_{115})\rangle\langle\rho(173_{168})\rangle \equiv \langle 173\rangle \bmod \xi.$$

Conventionally, we write ideals in Gothic script, e.g. $\mathfrak{a}$, with subscripts denoting their norms (how to define the norm of an ideal can be found in standard textbooks). We will just note that where representations exist, $N(\langle\rho\rangle) = |N(\rho)|$.

We can also write factorizations in terms of ideals, even though representations don't exist. For example, $f(r) \equiv 0 \bmod 223$ has

$$\langle 223\rangle = \mathfrak{a}_{223}\mathfrak{a}'_{223}\mathfrak{a}''_{223},$$

where

$$\mathfrak{a}_{223} = \langle\rho(223_{170})\rangle,\ \mathfrak{a}'_{223} = \langle(X-79), 223\rangle \text{ and } \mathfrak{a}''_{223} = \langle(X-196), 223\rangle.$$

In the one root case, we have to consider q of the form $q_1Y + q_2p \bmod f$ for arbitrary polynomials q_1, q_2, where $(X-r)Y \equiv f \bmod p$. Now

$$q_1 Y + q_2 p \;\equiv\; q_3\rho(p_*^2), \quad \text{where} \quad q_3 \;=\; q_1\tau(p_*^2) + q_2\rho(p_r) \bmod f.$$

We therefore have $\langle Y, p\rangle = \langle \rho(p_*^2)\rangle$.

For example, in the previous section, we saw that $f(r) \equiv 0 \bmod 239$ has the single root 45. We therefore have

$$\langle 239\rangle \;=\; \mathfrak{a}_{239}\mathfrak{a}'_{57121}, \quad \text{where} \quad \mathfrak{a}_{239} \;=\; \langle\rho(239_{45})\rangle,\ \mathfrak{a}'_{57121} \;=\; \langle\rho(239_*^2)\rangle.$$

Finally, we return to the original example of non-unique factorization. Recall that $g = 104X^2+30X+1749$, $h = 5X^2+2X+85$, that $gh \equiv 183 \bmod \xi$ and that g could be thought of as $\rho(3_0 61_6 61_{16})$, and h as $\rho(3_*^2 61_{38})$. We can now write

$$\langle 3\rangle \;=\; \mathfrak{a}_3\mathfrak{a}'_9, \quad \text{where} \quad \mathfrak{a}_3 \;=\; \langle X-0, 3\rangle,\ \mathfrak{a}'_9 = \langle X^2+X+2, 3\rangle,$$

since $(X-0)(X^2+X+2) \equiv 0 \bmod 3$. Similarly,

$$\langle 61\rangle \;=\; \mathfrak{b}_{61}\mathfrak{b}'_{61}\mathfrak{b}''_{61},$$

where

$$\mathfrak{b}_{61} \;=\; \langle X-6, 61\rangle,\ \mathfrak{b}'_{61} \;=\; \langle X-16, 61\rangle \;\text{ and }\; \mathfrak{b}''_{61} \;=\; \langle X-38, 61\rangle.$$

We have $\langle g\rangle = \mathfrak{a}_3\mathfrak{b}_{61}\mathfrak{b}'_{61}$ and $\langle h\rangle = \mathfrak{a}'_9\mathfrak{b}''_{61}$; so

$$\langle gh\rangle \;=\; \mathfrak{a}_3\mathfrak{b}_{61}\mathfrak{b}'_{61}\mathfrak{a}'_9\mathfrak{b}''_{61} \;=\; \mathfrak{a}_3\mathfrak{a}'_9\mathfrak{b}_{61}\mathfrak{b}'_{61}\mathfrak{b}''_{61} \;=\; \langle 3\rangle\langle 61\rangle \;=\; \langle 183\rangle.$$

5 Parts 2 and 3

Part 2 of this series will look at the proportion of prime / root combinations p_r for a particular f that have a representation, how some polynomials are related to each other, and how all this is related to the algebraic number theory concept of class number.

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

6 References

Barrucand, P., Williams H. C., Baniuk, L. (1976) A computational technique for determining the class number of a pure cubic field, *Mathematics of Computation*, vol. 30 no. 134, pp. 312–323.

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

Cohn, H. (1957) A Numerical Study of Dedekind's Cubic Class Number Formula, *Journal of Research of the National Bureau of Standards*, vol. 59 no. 4, pp. 265–271.

Conrad, K. (2003) Factoring after Dedekind. Available at `www.math.uconn.edu/~kconrad/blurbs/gradnumthy/dedekindf.pdf`.

Solution 282.5 – Determinant

Compute

$$\Lambda(n,\lambda) \;=\; \det\begin{bmatrix} \lambda & -1 & \dots & -1 & -1 \\ -1 & \lambda & \dots & -1 & -1 \\ \dots & \dots & \dots & \dots & \dots \\ -1 & -1 & \dots & \lambda & -1 \\ -1 & -1 & \dots & -1 & \lambda \end{bmatrix},$$

where n is the number of rows in the matrix. Hence or otherwise prove that $\Lambda(n-1,n-1) = n^{n-2}$.

Tommy Moorhouse

A useful identity. For any matrix A the problem of finding the determinant of e^A can be reduced to the problem of finding a related trace using

$$\det e^A \;=\; \exp(\operatorname{Tr} A).$$

This identity can be proved in stages, starting with the case of diagonal A. Here matrix functions will be considered to be defined by their formal power series expansions.

Deconstructing $\Lambda(N,\lambda)$. We can write $\Lambda(N,\lambda) = (1+\lambda)\mathbb{I} - \mathbb{U}$ where $\mathbb{I}$ is the identity matrix and $\mathbb{U}$ is the matrix with all its entries equal to unity. We want this to be e^A. Taking logs we get

$$\begin{aligned} A &= \log\left((1+\lambda)\left(\mathbb{I} - \frac{1}{1+\lambda}\mathbb{U}\right)\right) \\ &= \log(1+\lambda)\mathbb{I} + \log\left(\mathbb{I} - \frac{1}{1+\lambda}\mathbb{U}\right) \\ &= \log(1+\lambda)\mathbb{I} - \sum_{k=1}^{\infty} \frac{1}{k(1+\lambda)^k}\mathbb{U}^k \end{aligned}$$

using the matrix version of the Taylor series of $\log(1-x)$. Now it is easy to see that $\mathbb{U}^k = N^{k-1}\mathbb{U}$ for $k \geq 1$ so we find

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{1}{k(1+\lambda)^k}\mathbb{U}^k &= \frac{1}{N}\sum_{k=1}^{\infty} \frac{N^k}{k(1+\lambda)^k}\mathbb{U} \\ &= -\frac{1}{N}\log\left(1 - \frac{N}{1+\lambda}\right)\mathbb{U}. \end{aligned}$$

Taking the trace. We have found that

$$A \;=\; \log(1+\lambda)\mathbb{I} + \frac{1}{N}\log\left(1-\frac{N}{1+\lambda}\right)\mathbb{U};$$

so taking the trace gives

$$\begin{aligned}\operatorname{Tr} A \;&=\; N\left(\log(1+\lambda)+\frac{1}{N}\log\left(1-\frac{N}{1+\lambda}\right)\right)\\ &=\; \log\left((1+\lambda)^{N-1}(1+\lambda-N)\right).\end{aligned}$$

Substituting $N = n-1$, $\lambda = n-1$ we find

$$\Lambda(n-1,n-1) \;=\; \exp(\operatorname{Tr} A) \;=\; n^{n-2},$$

as required.

Peter Fletcher

Recall that the determinant of an $n\times n$ matrix is equal to the product of its n eigenvalues and that an upper triangular matrix has all its eigenvalues down the leading diagonal.

We may reduce the given matrix to an upper triangular one by elementary row and column operations.

Step 1. Subtract the $(n-1)^{\text{th}}$ row from the n^{th}. This gives

$$\begin{pmatrix} \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \lambda & -1 & -1 & -1 & -1 \\ \cdots & -1 & \lambda & -1 & -1 & -1 \\ \cdots & -1 & -1 & \lambda & -1 & -1 \\ \cdots & -1 & -1 & -1 & \lambda & -1 \\ \cdots & 0 & 0 & 0 & -1-\lambda & \lambda+1 \end{pmatrix}.$$

Step 2. Add the n^{th} column to the $(n-1)^{\text{th}}$. This gives

$$\begin{pmatrix} \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \lambda & -1 & -1 & -2 & -1 \\ \cdots & -1 & \lambda & -1 & -2 & -1 \\ \cdots & -1 & -1 & \lambda & -2 & -1 \\ \cdots & -1 & -1 & -1 & \lambda-1 & -1 \\ \cdots & 0 & 0 & 0 & 0 & \lambda+1 \end{pmatrix}.$$

We now repeat steps 1 and 2 on the $(n-1)\times(n-1)$ submatrix formed by the first $(n-1)$ rows and columns.

Step 3. Subtract the $(n-2)^{\text{th}}$ row from the $(n-1)^{\text{th}}$. This gives

$$\begin{pmatrix}
\ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\cdots & \lambda & -1 & -1 & -2 & -1 \\
\cdots & -1 & \lambda & -1 & -2 & -1 \\
\cdots & -1 & -1 & \lambda & -2 & -1 \\
\cdots & 0 & 0 & -1-\lambda & \lambda+1 & 0 \\
\cdots & 0 & 0 & 0 & 0 & \lambda+1
\end{pmatrix}.$$

Step 4. Add the $(n-1)^{\text{th}}$ column to the $(n-2)^{\text{th}}$. This gives

$$\begin{pmatrix}
\ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\cdots & -1 & -1 & -3 & -2 & -1 \\
\cdots & \lambda & -1 & -3 & -2 & -1 \\
\cdots & -1 & \lambda & -3 & -2 & -1 \\
\cdots & -1 & -1 & \lambda-2 & -2 & -1 \\
\cdots & 0 & 0 & 0 & \lambda+1 & 0 \\
\cdots & 0 & 0 & 0 & 0 & \lambda+1
\end{pmatrix}.$$

Carrying on in this way, after $2n-4$ steps we eventually get to

$$\begin{pmatrix}
\lambda & -(n-1) & -(n-2) & -(n-3) & -(n-4) & \cdots \\
-1 & \lambda-(n-2) & -(n-2) & -(n-3) & -(n-4) & \cdots \\
0 & 0 & \lambda+1 & 0 & 0 & \cdots \\
0 & 0 & 0 & \lambda+1 & 0 & \cdots \\
0 & 0 & 0 & 0 & \lambda+1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{pmatrix}.$$

Step $2n-3$. Subtract the 1^{st} row from the 2^{nd}. This gives

$$\begin{pmatrix}
\lambda & -(n-1) & -(n-2) & -(n-3) & -(n-4) & \cdots \\
-1-\lambda & \lambda+1 & 0 & 0 & 0 & \cdots \\
0 & 0 & \lambda+1 & 0 & 0 & \cdots \\
0 & 0 & 0 & \lambda+1 & 0 & \cdots \\
0 & 0 & 0 & 0 & \lambda+1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{pmatrix}$$

Step $2n-2$. Add the 2^{nd} column to the 1^{st}. This gives

$$\begin{pmatrix} \lambda-(n-1) & -(n-1) & -(n-2) & -(n-3) & -(n-4) & \cdots \\ 0 & \lambda+1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & \lambda+1 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \lambda+1 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \lambda+1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

We have $\lambda-(n-1)$ and $n-1$ copies of $\lambda+1$ on the leading diagonal. Therefore the determinant of our matrix is

$$\Lambda(n,\lambda) = (\lambda-n+1)(\lambda+1)^{n-1}.$$

We can now write down

$$\Lambda(n-1,n-1) = (n-1-n+1+1)(n-1+1)^{n-1-1} = n^{n-2}.$$

Stuart Walmsley

This is similar to Problem 261.6, for which I gave a solution in M500 263 pages 1–5. In fact, the solution of the present problem can be found directly, leading to

$$\Lambda(n,\lambda) \;=\; (\lambda-n+1)(\lambda+1)^{n-1};$$

whence

$$\Lambda(n-1,n-1) \;=\; ((n-1)-(n-1)+1))((n-1)+1)^{n-2},$$

giving

$$\Lambda(n-1,n-1) \;=\; n^{n-2},$$

which is the result to be proved.

The solution took advantage of the symmetry of the matrix and used the methods of group theory. In general terms, the expanded determinant is a polynomial of degree n in λ. As such, it has n distinct roots, r_1, r_2, $\ldots$, r_n, and the polynomial may be written

$$(\lambda-r_1)(\lambda-r_2)\ldots(\lambda-r_n).$$

This, in turn, may be written as a determinant of the matrix

$$L(n,\lambda) \;=\; \left[\begin{array}{cccc} \lambda - r_1 & 0 & \dots & 0 \\ 0 & \lambda - r_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda - r_n \end{array}\right].$$

The two equivalent forms of the matrix can be related by an expression of the form

$$T\Lambda(n,\lambda)T^{-1} \;=\; L(n,\lambda),$$

where T is a matrix which specifies the transformation between the two forms. (Note that in this expression $\Lambda(n,\lambda)$ denotes the matrix, not the determinant.)

In the original problem, the form of T is precisely defined by the symmetry. In the present case, the repeated roots allow a range of equivalent forms. The original form degenerates to an acceptable version. To amplify these considerations, consider the case $n = 3$. Then

$$\Lambda(3,\lambda) \;=\; \det \left[\begin{array}{rrr} \lambda & -1 & -1 \\ -1 & \lambda & -1 \\ -1 & -1 & \lambda \end{array}\right].$$

Direct expansion gives

$$\Lambda(3,\lambda) \;=\; \lambda^3 - 3\lambda - 2.$$

It is easy to guess one of the roots and solve the resulting quadratic to give the factored form

$$\Lambda(3,\lambda) \;=\; (\lambda - 2)(\lambda + 1)^2.$$

The matrix has a threefold cyclic pattern which can be used to obtain T:

$$T \;=\; \frac{1}{\sqrt{3}} \left[\begin{array}{ccc} 1 & 1 & 1 \\ 1 & \omega & \omega^* \\ 1 & \omega^* & \omega \end{array}\right], \quad T^{-1} \;=\; \frac{1}{\sqrt{3}} \left[\begin{array}{ccc} 1 & 1 & 1 \\ 1 & \omega^* & \omega \\ 1 & \omega & \omega^* \end{array}\right],$$

where $\omega = \exp(2\pi i/3)$, $\omega^* = \exp(-2\pi i/3)$. Then

$$T\Lambda(3,\lambda)T^{-1} \;=\; \left[\begin{array}{ccc} \lambda - 2 & 0 & 0 \\ 0 & \lambda + 1 & 0 \\ 0 & 0 & \lambda + 1 \end{array}\right].$$

This may be generalized using the appropriate (complex) roots of unity. Because of the repeated roots, the form of T is not unique. An alternative is:

$$T = \begin{bmatrix} 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ -1/\sqrt{2} & 1/\sqrt{2} & 0 \\ -1/\sqrt{6} & -1/\sqrt{6} & 2/\sqrt{6} \end{bmatrix}.$$

The inverse of this matrix is its transpose.

This may be generalized to any number of dimensions and is referred to in the literature as the Schmidt orthogonalization procedure.

Reinhardt Messerschmidt

Let J and $\mathbf{1}$ be the all-1 matrix and column vector respectively, with their dimensions determined by the context. If n is a positive integer and λ, μ are complex numbers, let $X(n,\lambda,\mu)$ be the $n \times n$ matrix defined by

$$X(n,\lambda,\mu) = (\lambda-\mu)I + \mu J = \begin{bmatrix} \lambda & \mu & \dots & \mu & \mu \\ \mu & \lambda & \dots & \mu & \mu \\ \dots & \dots & \dots & \dots & \dots \\ \mu & \mu & \dots & \lambda & \mu \\ \mu & \mu & \dots & \mu & \lambda \end{bmatrix}.$$

We will use induction on n to show that

$$\det X(n,\lambda,\mu) = (\lambda-\mu)^{n-1}(\lambda+(n-1)\mu).$$

For the base case,

$$\det X(1,\lambda,\mu) = \lambda = (\lambda-\mu)^{1-1}(\lambda+(1-1)\mu).$$

For the inductive case, suppose $n \geq 2$ and

$$\det X(n-1,\lambda,\mu) = (\lambda-\mu)^{n-2}(\lambda+(n-2)\mu).$$

We have

$$\det X(n,\lambda,\mu) = \det \begin{bmatrix} X(n-1,\lambda,\mu) & \mu\mathbf{1} \\ \mu\mathbf{1}^T & \lambda \end{bmatrix}.$$

Adding $-\mu/\lambda$ times the n-th row to the 1st, 2nd, …, $(n-1)$-th rows,

$$\det X(n,\lambda,\mu) = \det \begin{bmatrix} X\left(n-1, \dfrac{\lambda^2-\mu^2}{\lambda}, \dfrac{\mu(\lambda-\mu)}{\lambda}\right) & \mathbf{0} \\ \mu\mathbf{1}^T & \lambda \end{bmatrix}.$$

Expanding by the last column,

$$\det X(n,\lambda,\mu) \;=\; \lambda \cdot \det X\left(n-1, \frac{\lambda^2-\mu^2}{\lambda}, \frac{\mu(\lambda-\mu)}{\lambda}\right).$$

By the inductive hypothesis,

$$\begin{aligned}\det X(n,\lambda,\mu) \;&=\; \lambda \cdot \left(\frac{(\lambda+\mu)(\lambda-\mu)}{\lambda} - \frac{\mu(\lambda-\mu)}{\lambda}\right)^{n-2} \\ &\qquad\cdot \left(\frac{(\lambda+\mu)(\lambda-\mu)}{\lambda} + (n-2)\frac{\mu(\lambda-\mu)}{\lambda}\right) \\ &=\; (\lambda-\mu)^{n-1}(\lambda+(n-1)\mu),\end{aligned}$$

which completes the induction. It follows that

$$\begin{aligned}\det \Lambda(n,\lambda) \;&=\; \det X(n,\lambda,-1) \;=\; (\lambda+1)^{n-1}(\lambda-n+1), \\ \det \Lambda(n-1,n-1) \;&=\; (n-1+1)^{n-1-1}\cdot 1 \;=\; n^{n-2}.\end{aligned}$$

Significance

Readers familiar with graph theory will recognize n^{n-2} as Cayley's formula for the number of spanning trees in the complete graph K_n, and $\Lambda(n-1,n-1)$ as an $(n-1)\times(n-1)$ principal submatrix of the Laplacian of K_n. We have therefore shown that the number of spanning trees in K_n is equal to the determinant of this submatrix. This is a special case of Kirchhoff's matrix-tree theorem, see section 1.3.5 in *Spectra of Graphs* by A. E. Brouwer & W. H. Haemers.

Problem 284.1 – Squares

Show that if a positive integer N can be expressed as $N = a^2+kb^2 = c^2+kd^2$ with a, b, c, d, k integers, $a \neq c$ and $k \geq 2$, then N must be composite.

Problem 284.2 – 13 cards

A standard pack of 52 playing cards is shuffled and dealt into 13 piles of four. Is it always possible to select one card from each pile so that the chosen cards consist of 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A, not necessarily of the same suit?

Solution 281.2 – Hours

> Four 'hour positions' are chosen at random on a standard clock face. What is the probability that, taken together, they define (a) a point, (b) a line, (c) a triangle, (d) a quadrilateral?

Peter Fletcher

Ignoring repetitions, there are 12^4 ways of picking four hour positions on a standard clock face.

(a) If the four hour positions are to define a point, then there are 12 ways of choosing the first position and we have 1 way of choosing each of the second, third and fourth positions. Therefore the probability that the four hour positions define a point is $12/12^4 = 1/1728$.

(b) If the four hour positions are to define a line then there are 12 ways of choosing the first position. Then we can choose a second position in 11 ways and the third and fourth in each of 2 ways; or we can choose the first position a second time in 1 way, the third in 11 ways and the fourth in 2 ways; or we can choose the first position a second and third time in 1 way and the fourth in 11 ways. In other words, the total number of ways of defining a line, including repetitions, is $12\cdot 11\cdot 2\cdot 2+12\cdot 1\cdot 11\cdot 2+12\cdot 1\cdot 1\cdot 11 = 924$. Therefore the probability that the four hour positions define a line is $924/12^4 = 77/1728$.

(c) If the four hour positions are to define a triangle then there are 12 ways of choosing the first position. Then we can choose the second position in 11 ways, the third in 10 ways and the fourth in 3 ways; or we can choose the second position in 11 ways, the third in 2 ways and the fourth in 10 ways; or we can choose the second position in 1 way, the third in 11 ways and the fourth in 10 ways. In other words, the total number of ways of defining a triangle is $12 \cdot 11 \cdot 10 \cdot 3 + 12 \cdot 11 \cdot 2 \cdot 10 + 12 \cdot 1 \cdot 11 \cdot 10 = 7920$. Therefore the probability that the four hour positions define a triangle is $7920/12^4 = 55/144$.

(d) If these four hour positions are to define a quadrilateral, then there are 12 ways of choosing the first position, 11 ways of choosing the second, 10 ways of choosing the third are 9 ways of choosing the fourth; so $12 \cdot 11 \cdot 10 \cdot 9 = 11880$ in all. Therefore the probability that the four hour positions define a quadrilateral is $11880/12^4 = 55/96$.

As a check,

$$\frac{1}{1728} + \frac{77}{1728} + \frac{55}{144} + \frac{55}{96} \;=\; 1,$$

so we have covered all possibilities.

Reinhardt Messerschmidt

The problem can be generalized to:

> Given positive integers m, n, k with $k \leq m$, what is the probability that a randomly chosen n-element $\{1, 2, \ldots, m\}$-valued sequence has k distinct elements?

The original problem is the case $m = 12$, $n = 4$ and $k \in \{1, 2, 3, 4\}$.

Let $X_{m,n}$ be the set of all n-element $\{1, 2, \ldots, m\}$-valued sequences, let $X_{m,n,k}$ be the set of all $x \in X_{m,n}$ with k distinct elements, and let $|A|$ denote the number of elements in a set A. If we can find $|X_{m,n,k}|$, then the answer to the general problem is

$$\frac{|X_{m,n,k}|}{|X_{m,n}|} \;=\; \frac{|X_{m,n,k}|}{m^n}.$$

Let $S(n, k)$ be the number of partitions of an n-element set into k subsets. This is known as a *Stirling number of the second kind.* Every $x \in X_{m,n,k}$ can be constructed as follows:

- Partition the set of n 'slots' in x into k subsets. This can be done in $S(n, k)$ ways.
- Fill the slots in the first subset with an element from $\{1, 2, \ldots, m\}$. This can be done in m ways.
- Fill the slots in the second subset with an element from $\{1, 2, \ldots, m\}$ that has not been used so far. This can be done in $m - 1$ ways.
- ...
- Fill the slots in the k-th subset with an element from $\{1, 2, \ldots, m\}$ that has not been used so far. This can be done in $m - k + 1$ ways.

It follows that

$$|X_{m,n,k}| \;=\; S(n, k) \cdot m \cdot (m - 1) \cdots (m - k + 1) \;=\; S(n, k)\frac{m!}{(m - k)!}.$$

It remains for us to find $S(n, k)$. There is only one way to partition an n-element set into 1 subset, and only one way to partition it into n subsets; therefore

$$S(n, 1) \;=\; 1, \qquad S(n, n) \;=\; 1. \tag{$*$}$$

If $n, k \geq 2$, then every partition of an n-element set into k subsets can be constructed as follows:

- Partition $n-1$ of the elements into k subsets, and add the n-th element to one of the k subsets. This can be done in $k \cdot S(n-1,k)$ ways.
- Alternatively, partition $n-1$ of the elements into $k-1$ subsets, and create a k-th subset consisting of the n-th element on its own. This can be done in $S(n-1,k-1)$ ways.

It follows that

$$S(n,k) \;=\; k \cdot S(n-1,k) + S(n-1,k-1). \tag{$**$}$$

The boundary conditions in $(*)$ and the recurrence relation in $(**)$ allow us to find $S(n,k)$. For the original problem, we need

$$\begin{aligned} S(3,2) &= 2 \cdot S(2,2) + S(2,1) = 2 \cdot 1 + 1 = 3,\\ S(4,2) &= 2 \cdot S(3,2) + S(3,1) = 2 \cdot 3 + 1 = 7,\\ S(4,3) &= 3 \cdot S(3,3) + S(3,2) = 3 \cdot 1 + 3 = 6. \end{aligned}$$

The answer to the original problem is

$$\begin{aligned} \frac{|X_{12,4,1}|}{12^4} &= \frac{1 \cdot 12}{12^4} = \frac{1}{1728} \approx 0.0006,\\ \frac{|X_{12,4,2}|}{12^4} &= \frac{7 \cdot 12 \cdot 11}{12^4} = \frac{77}{1728} \approx 0.0446,\\ \frac{|X_{12,4,3}|}{12^4} &= \frac{6 \cdot 12 \cdot 11 \cdot 10}{12^4} = \frac{660}{1728} \approx 0.3819,\\ \frac{|X_{12,4,4}|}{12^4} &= \frac{1 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{12^4} = \frac{990}{1728} \approx 0.5729. \end{aligned}$$ □

Problem 284.3 – Characteristic polynomial

Show that a square matrix is a root of its characteristic polynomial. In other words, if M is an $n \times n$ matrix, and

$$P_M(x) \;=\; \det(xI_n - M) \;=\; \sum_{i=0}^{n} a_i x^i$$

is its characteristic polynomial, show that

$$P_M(M) \;=\; \sum_{i=0}^{n} (a_i I_n) M^i \;=\; 0_n,$$

where I_n is the $n \times n$ identity matrix, and 0_n is the $n \times n$ all-zeros matrix.

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?

Peter Fletcher

The first thing to do is to count the number of dice-throws possible.

If the host shows a 1, then we know that the two hidden dice must show (1,1), only one possibility.

If he shows a 2, then we know that the two hidden dice must show (1,1), (1,2), (2,1) or (2,2), four possibilities.

If he shows a 3, then we know that the two hidden dice must show (1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2) or (3,3), nine possibilities.

If he shows a 4, then we know that the two hidden dice must show (1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4), (3,1), (3,2), (3,3), (3,4), (4,1), (4,2), (4,3) or (4,4), 16 possibilities.

We can see that the total number of possibilities increases as the square of the number on the die that the host shows. Therefore the total number of possible dice-throws is $1 + 4 + 9 + 16 + 25 + 36 = 91$.

From the above, we can count the number of times the value of the die that the host shows also appears on at least one of the two hidden dice.

If he shows a 1, there is one way that at least one of the hidden dice also shows a 1.

If he shows a 2, there are three ways that at least one of the hidden dice also shows a 2.

If he shows a 3, there are five ways that at least one of the hidden dice also shows a 3.

If he shows a 4, there are seven ways that at least one of the hidden dice also shows a 4.

We can see that the total number of possibilities increases as consecutive odd numbers. Therefore the probability that at least one of the two hidden dice shows the same value as that shown by the host is

$$\frac{1+3+5+7+9+11}{91} = \frac{36}{91}.$$

Emma Lehmer

Eddie Kent

In 2006 I wrote about Emma Lehmer [M500 **213** 16], who was born in 1906, and with crashing originality I called it '100 not out'. In fact Emma died in 2007. She was born Emma Trotskaia in Russia ('in a town with the lovely sounding name of Samara'), and moved to the USA for her higher education. There she married her tutor's son, Derrick H. Lehmer and they moved to Brown University where he got a Ph.D. and she (for university constitutional reasons) was restricted to an M.Sc. She was still able to write 56 papers in the area of number theory. When her husband died in 1991 she completed his unfinished research papers. Paul Halmos wrote *I want to be a Mathematician* in 1985, and in this he referred to Lehmer's translation of Pontryagin's *Topological Groups*. He called her Emma Lemma; this caught on.

Impact

Jeremy Humphries

I'm reading *No Middle Name*, the complete collected Jack Reacher short stories by Lee Child. Just come across this in the story 'Deep Down'.

> The guy in black weighed maybe one-ninety, and he was doing about two miles an hour. Reacher weighed two-fifty, and he was doing three miles an hour. Therefore closing speed was five miles an hour, and impact, should it happen, would involve some multiple of four hundred forty pounds a square inch.

Eh?

M500 Winter Weekend 2019

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

Florence Boot Hall, **Nottingham University**

Friday 4th – Sunday 6th January 2019.

The cost for the Weekend will be confirmed when booking opens at the end of September 2018. The cost includes accommodation and all meals from dinner on Friday to lunch on Sunday.

The Winter Weekend provides you with an opportunity to do some non-module-based, recreational maths with a friendly group of like-minded people. The relaxed and social approach delivers maths for fun. And as well as a complete programme of mathematical entertainments, on Saturday we will be running a pub quiz with Valuable Prizes.

Contents M500 284 – October 2018

04.00

Problem 284.4 – Factorial square

For positive integers p and q, define

$$F(p,q) \;=\; \frac{1}{q!}\prod_{j=1}^{p} j!.$$

(i) Show that $F(4n,2n)$ is always a square, or find a counter-example. For instance,

$$F(12,6) \;=\; 2!\,3!\,4!\,5!\;\,7!\,8!\,9!\,10!\,11!\,12! \;=\; 420505587390873600000^2.$$

(ii) With the exception of $F(1,1)=1$, show that $F(p,q)$ cannot be a square if p is odd. Or find another example.

(iii) Show that $F(14,9)$ and $F(18,7)$ are squares.

(iv) Prove the following, or find a counter-example. Apart from $F(14,9)$ and $F(18,7)$, if $F(2n,q)$ is a square, then $n-1 \le q \le n+1$.

Front cover The mono, di, tri and tetracubes. See M500 **182** for the pentacubes. And if someone provides me (TF) with the 166 hexacubes suitably encoded, I will put them on the cover of a future M500.