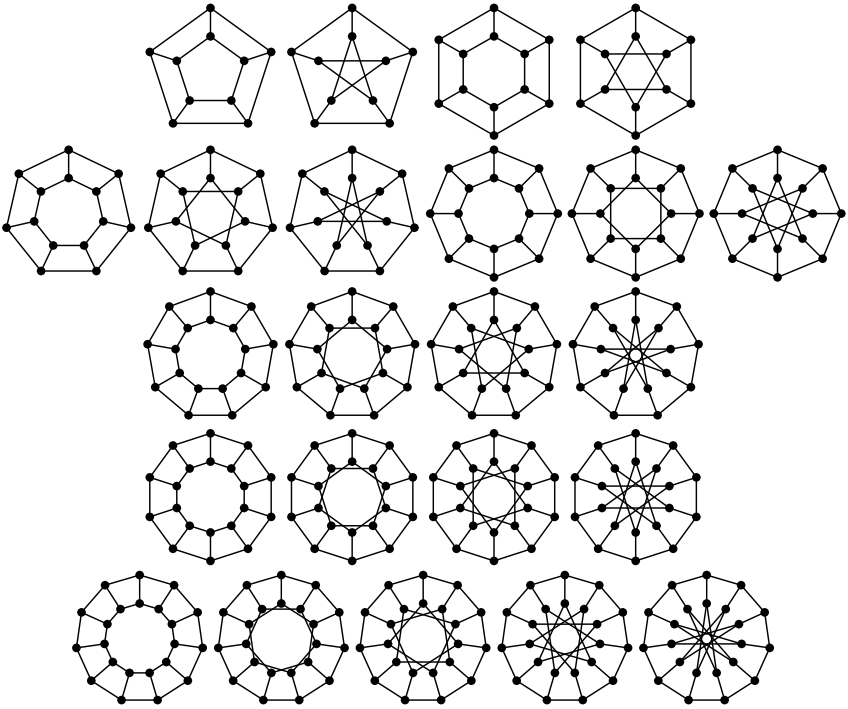
*

ISSN 1350-8539

M500

M500 273



The M500 Society and Officers

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

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

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

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

Advice to authors We welcome contributions to M500 on virtually anything related to mathematics and at any level from trivia to serious research. Please send material for publication to the Editor, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation.

Subscription renewal If your M500 Society membership expires at the end of 2016, you will receive a subscription renewal form either separately by email or, if you do not have an email address, on paper together with this magazine. Please follow the instructions on the form to renew your subscription.

Sophie Germain and Fermat's Last Theorem – II

Roger Thompson

Sophie Germain's Theorem

Sophie Germain's Theorem divides Fermat's Last Theorem for any prime exponent p into two cases:

Case 1: $x^p + y^p + z^p = 0$, where none of x, y, z is divisible by p.

Case 2: $x^p + y^p + z^p = 0$, where one of x, y, z is divisible by p.

Although she never actually proved Fermat's Last Theorem for a single exponent in both cases, she did prove it for many exponents in case 1. The theorem contains two conditions. The second of these has two alternative formulations, shown as 2a and 2b in the following.

Sophie Germain's theorem Let p be an odd prime. Suppose there exists an auxiliary prime q such that the following conditions hold.

1. $n^p \not\equiv p \bmod q$ for all integers n.

2a. q is of the form $2Np + 1$ for some integer N, and the set of distinct values of $x^p \bmod q$ contains no consecutive non-zero values.

2b. There exists a prime q such that for all pairwise relatively prime a, b and c such that $a^p + b^p + c^p \equiv 0 \bmod q$, q is a factor of abc.

Then there are no non-zero integers x, y, z such that $x^p + y^p + z^p = 0$ if none of x, y, z is divisible by p; i.e. case 1 of Fermat's Last Theorem is proven.

Sophie Germain's approach to condition 2a

Instead of dealing with N values one at a time, her idea is use a fixed (but unspecified) odd p and show that if there is a pair of pth powers mod $(2Np+1)$ that are consecutive, there are six algebraically distinct such pairs. She then shows that subject to certain conditions, it is possible to derive twelve distinct pth powers. Since there are $2Np$th powers $\bmod(2Np + 1)$, this immediately shows that consecutive pth powers $\bmod(2Np + 1)$ cannot exist for $N = 1, 2, 4, 5$, since these only have 2, 4, 8 or 10 pth powers $\bmod(2Np + 1)$. The conditions she needs are:

(i) N is not a multiple of 3. We have already seen that multiples of 3 are troublesome.

(ii) $n^p \not\equiv 2 \bmod (2Np+1)$ for all integers n. Since p is odd, this implies $n^p \not\equiv \pm 2 \bmod (2Np + 1)$.

Since this has to hold for condition 2a to apply (for otherwise 1 and 2 would be consecutive pth powers), it is no extra restriction; rather she is exploring whether it is sufficient for condition 2a to apply. Finding the exceptions is

straightforward. If $n^p \equiv 2 \bmod (2Np+1)$ for some integer n, we must have $2^{2N} \equiv 1 \bmod (2Np+1)$ (by raising both sides to the $2N$th power). All we need to do is factorize $2^{2N}-1$ and see for what factors of the form $2Nx+1$, x is prime.

N	$2^{2N}-1$	Factors	Excluded p
1	3	$2\times 1+1$	None
2	15	$3\times(4\times 1+1)$	None
4	255	$3\times 5\times(8\times 2+1)$	2
5	1023	$3\times(10\times 1+1)(10\times 3+1)$	3
7	16383	$3\times(14\times 3+1)(14\times 9+1)$	3
8	65535	$3\times 5\times(16\times 1+1)(16\times 16+1)$	None

The following arguments are taken from Sophie Germain's unpublished manuscript 'Remarque sur l'impossibilité de satisfaire en nombres entiers à l'équation $x^p+y^p=z^p$'. Her mathematical style here is very terse, so while the arguments are as presented there, they have been expanded upon (at length, in some cases).

We first show how the above conditions arise. Let v be a primitive $2N$th root of 1 modulo q, where $q=2Np+1$. Then by definition, $v^{2N} \equiv 1 \bmod q, v^N \equiv -1 \bmod q$. Since $q-1$ is divisible by $2Np$, primitive $2Np$th roots of 1 modulo q exist. Let a be such a root. Then a^p must be a primitive $2N$th root of 1 modulo q, since the set $\{1, a^p, a^{2p}, \ldots, a^{2N(p-1)}\}$ consists of every pth element of $\{1, a, a^2, \ldots, a^{2Np-1}\}$, which are all distinct. We therefore have $v \equiv a^p \bmod q$ for some a.

Suppose condition 2a is not satisfied, so that $v^S \equiv v^T + 1 \bmod q$ for some $S, T < 2N$, with $v^S \not\equiv 0 \bmod q$, $v^T \not\equiv 0 \bmod q$. Since q is prime, v^{-T} exists, so we can multiply to give $v^{S-T} \equiv 1 + v^{-T} \equiv 1 + v^{2N-T} \bmod q$. Similarly, v^{-S} exists, so $1 \equiv v^{T-S} + v^{-S} \equiv v^{T-S} - v^{N-S} \bmod q$, i.e. $v^{T-S} \equiv v^{N-S} + 1 \bmod q$. Repeating with a further three similar operations gives the six relations:

(a) $1 + v^T \equiv v^S \bmod q$, (b) $1 + v^{2N-T} \equiv v^{S-T} \bmod q$,
(c) $1 + v^{N-S} \equiv v^{T-S} \bmod q$, (d) $1 + v^{N+S} \equiv v^{N+T} \bmod q$,
(e) $1 + v^{N+S-T} \equiv v^{N-T} \bmod q$, (f) $1 + v^{N+T-S} \equiv v^{2N-S} \bmod q$.

We now examine the cases where these six relations can be reduced. Since the relations are symbolic, we only have to compare (a) with (b) to (f).

1. (a) and (b) are equivalent: $T \equiv 2N - T \bmod 2N$ ($2N$ rather than q, since we are dealing with the exponents, which run from 0 to $2N-1$), and $S \equiv S - T \bmod 2N$, so $T = 0$, reducing the six relations to three:

(g) $2 \equiv v^S \bmod q$, (h) $1 + v^{N-S} \equiv v^{2N-S} \bmod q$,
(i) $1 + v^{N+S} \equiv v^N \bmod q$.

Similarly, the equivalence of (a) and (d), or the equivalence of (a) and (f) both lead to $2 \equiv v^X \bmod q$ for a particular X. By requiring $n^p \not\equiv 2 \bmod q$ for all integers n, these reductions cannot occur, since we have already shown that v is a power of p.

2. (a) and (c) are equivalent: $T \equiv N - S \bmod 2N$, $S \equiv T - S \bmod 2N$, giving $2S \equiv T \bmod 2N$, $3S \equiv N \bmod 2N$. The solution $T = 0$, $S = N$ is disallowed, since this would imply $v^S \equiv 2 \bmod q$, so N must be a multiple of 3 if this reduction is allowed. The equivalence of (a) and (e) gives rise to the same expressions.

If none of the right hand side powers of v equals one of the left hand side powers of v, we have twelve distinct pth powers. We now need to see what happens if one of the right hand side powers of v equals one of the left hand side powers of v. Since the relations are symbolic, we only have to compare the right hand side of (a), i.e. v^S with the v powers on the left hand sides of (b) to (f).

If $S \equiv N - S \bmod 2N$ (from (c)), we get $(1 + v^T)^2 \equiv 1 + 2v^T + v^{2T} \equiv v^{2S} \equiv v^N \equiv -1 \bmod q$, so $-v^{2T} \equiv 2(1 + v^T) \equiv 2v^S \bmod q$, using $1 + v^T \equiv v^S \bmod q$ from (a). Multiplying by v^{2N-S}, we get $2 \equiv -v^{2T+2N-S} \equiv v^{2T+N-S} \bmod q$. Since we have already excluded 2 as a pth power, we cannot have $S \equiv N - S \bmod 2N$.

If $S \equiv N + S \bmod 2N$ (from (d)), we get $N \equiv 0 \bmod 2N$, which is impossible.

If $S \equiv N + S - T \bmod 2N$ (from (e)), we get $N \equiv T \bmod 2N$, leading to $1 + v^T \equiv 1 - 1 \equiv 0 \bmod 2N$, but from (a), this would imply $v^S \equiv 0 \bmod 2N$, which is not allowed.

If $S \equiv 2N - T \bmod 2N$ (from (b)), the six relations become:

(a1) $1 + v^{2N-S} \equiv v^S \bmod q$, (b1) $1 + v^S \equiv v^{2S} \bmod q$,
(c1) $1 + v^{N-S} \equiv v^{2N-2S} \bmod q$, (d1) $1 + v^{N+S} \equiv v^{N-S} \bmod q$,
(e1) $1 + v^{N+2S} \equiv v^{N+S} \bmod q$, (f1) $1 + v^{N-2S} \equiv v^{2N-S} \bmod q$.

From (e1), (d1), (c1), v^{N+2S}, v^{N+S}, v^{N-S}, v^{2N-2S} are consecutive integers modulo q, x to $x + 3$ say. From (f1), (a1), (b1), v^{N-2S}, v^{2N-S}, v^S, v^{2S} are consecutive integers modulo q, y to $y + 3$ say.

If $S \equiv N + T - S \bmod 2N$ (from (f)), the six relations become:

(a2) $1 + v^{N+2S} \equiv v^S \bmod q$, (b2) $1 + v^{N-2S} \equiv v^{N-S} \bmod q$,
(c2) $1 + v^{N-S} \equiv v^{N+S} \bmod q$, (d2) $1 + v^{N+S} \equiv v^{2S} \bmod q$,
(e2) $1 + v^{2N-S} \equiv v^{2N-2S} \bmod q$, (f2) $1 + v^S \equiv v^{2N-S} \bmod q$.

From (a2), (f2), (e2), $v^{N+2S}, v^S, v^{2N-S}, v^{2N-2S}$ are consecutive integers modulo q, y to $y+3$ say. From (b2), (c2), (d2), $v^{N-2S}, v^{N-S}, v^{N+S}, v^{2S}$ are

consecutive integers modulo q, x to $x+3$ say. In the x cases for both the above sets of relations, we have $(x+1)(x+2) \equiv v^{2N} \equiv 1 \bmod q$, $x(x+3) \equiv -1 \bmod q$. Similarly, $(y+1)(y+2) \equiv 1 \bmod q$, $y(y+3) \equiv -1 \bmod q$, so in further analysis, we can treat x, y similarly.

Let $z \equiv x+1 \bmod q$. Then $x+2 \equiv z^{-1} \bmod q$, and $2x+3 \equiv z+z^{-1} \bmod q$. So $(2x+3)^2 \equiv (z+z^{-1})^2 \equiv z^2+z^{-2}+2 \equiv (x+1)^2+(x+2)^2+2 \equiv 2x^2+6x+7 \bmod q$. Now $2(x+1)(x+2) \equiv 2 \equiv 2x^2+6x+4 \bmod q$, so $(2x+3)^2 \equiv 5 \bmod q$. Similarly, $(2y+3)^2 \equiv 5 \bmod q$, so either $x \equiv y \bmod q$ (impossible, since (a) to (f) are distinct), or $2x+3 \equiv -(2y+3) \bmod q$, giving $y \equiv -x-3 \bmod q$, since q is odd.

The elements which are powers of v in (a1) to (f1), (a2) to (f2), which are all pth powers, are therefore $\pm x$, $\pm(x+1)$, $\pm(x+2)$, $\pm(x+3)$ (Note that Laubenbacher and Pengelley (2010) p. 28 assumes that six distinct pairs implies twelve distinct elements—not so, there are only eight).

Rearranging $(x+1)(x+2) \equiv 1 \bmod q$, we get $x(x+1) \equiv -(2x+1) \bmod q$. Since $x, x+1$ and -1 are pth powers, so is $2x+1$. If we assume $2x+1 \equiv x+k \bmod q, 0 \le k \le 3$, then $x+3-k \equiv 2 \bmod q$, so one of $x, x+1, x+2, x+3$ is excluded, so the assumption is invalid. We assume $2x+1 \equiv -(x+k) \bmod q, 0 \le k \le 3$, and use the identity $x(x+3) \equiv x^2+3x \equiv -1 \bmod q$, i.e. $3x \equiv -x^2-1 \bmod q$.

If $2x+1 \equiv -x \bmod q$, $x^2 \equiv 0 \bmod q$, impossible. If $2x+1 \equiv -(x+1) \bmod q$, $x^2 \equiv 1 \bmod q$, giving $x \equiv \pm 1 \bmod q$, with $x+1 \equiv 2 \bmod q$, or $x+3 \equiv 2 \bmod q$, both forbidden (this corrects a mistake in the manuscript). If $2x+1 \equiv -(x+2) \bmod q$, $3x \equiv -3 \bmod q$, i.e. $x \equiv -1 \bmod q$, since $q \neq 3$. But then $x+3 \equiv 2 \bmod q$, forbidden (this corrects a mistake in the manuscript). If $2x+1 \equiv -(x+3) \bmod q$, $3x \equiv -4 \bmod q \equiv -x^2-1 \bmod q$ from above, giving $x^2 \equiv 3 \bmod q$. We therefore have $x^2+2(3x+4) \equiv 3 \bmod q$, or $(x+3)^2 \equiv 4 \bmod q$, giving $x+3 \equiv \pm 2 \bmod q$, both of which are forbidden.

Since ± 1 are pth powers, we have (at least) the following twelve distinct elements: ± 1, $\pm x$, $\pm(x+1)$, $\pm(x+2)$, $\pm(x+3)$, $\pm(2x+1)$. We have therefore shown that consecutive pth powers modulo $2Np+1$ cannot exist for $N = 1$, 2, 4, 5, since each of these has less than twelve distinct pth powers, so we have proved case 1 of Fermat's Last Theorem for (at least) all $p < 197$ apart from $p = 47$, 59, 61, 167.

Sophie Germain's proofs for $N = 7, 8$, only found in unpublished manuscripts, were independently rediscovered in 1908 by Dickson (see Laubenbacher and Pengelley (2010) section 3.3.2). While they have much in common, some arguments are sufficiently different to warrant separate sections for the proofs.

Sophie Germain's proof for $N = 7$

The techniques and use of variables from the previous section are also used here. We will also need the following:

$$(1-v)\sum_{k=0}^{2N-1} v^k \;\equiv\; \sum_{k=0}^{2N-1} v^k - v\sum_{k=0}^{2N-1} v^k \;\equiv\; 1 - v^{2N} \;\equiv\; 0 \bmod q.$$

Since $v \not\equiv 1 \bmod q$, we have $\sum_{k=0}^{2N-1} v^k \equiv 0 \bmod q$. If $d > 1$ is a factor of $2N$,

$$\begin{aligned}\sum_{k=0}^{2N-1} v^k &\equiv (1 + v + v^2 + \cdots + v^{d-1})(1 + v^d + v^{2d} + \cdots + v^{2N-d}) \bmod q \\ &\equiv (v^d - 1)(v-1)^{-1}(1 + v^d + v^{2d} + \cdots + v^{2N-d}) \bmod q.\end{aligned}$$

Since v is a primitive $2N$th root of 1 modulo q, and $1 < d < 2N$, we have $v^d \not\equiv 1 \bmod q$, and $v \not\equiv 1 \bmod q$; so $\sum_{k=0}^{2N/d-1} v^{dk} \equiv 0 \bmod q$. If d is even $= 2e$ say, we have $\sum_{k=0}^{N/e-1} v^{2ek} \equiv 0 \bmod q$, giving $\sum_{k=0}^{N-1} (v^{2f})^k \equiv 0 \bmod q$ for any f, regardless of whether v^f is or is not a primitive $2N$th root of 1 modulo q.

She examines the combinations of odd and even values of S and T in the powers of v for the six relations explored earlier:

(a) $1 + v^T \equiv v^S \bmod q$, (b) $1 + v^{2N-T} \equiv v^{S-T} \bmod q$,
(c) $1 + v^{N-S} \equiv v^{T-S} \bmod q$, (d) $1 + v^{N+S} \equiv v^{N+T} \bmod q$,
(e) $1 + v^{N+S-T} \equiv v^{N-T} \bmod q$, (f) $1 + v^{N+T-S} \equiv v^{2N-S} \bmod q$.

She first examines the case where none of the right hand side powers of v equals one of the left hand side powers of v. In what follows, exp-even/odd means the exponent of v is even/odd. In the table below summarizing these combinations, the two entries represent the left and right hand sides of each equivalence. For $N = 7$, this gives the following.

	S even, T even	S even, T odd	S odd, T even	S odd, T odd
(a)	exp-even, exp-even	exp-odd, exp-even	exp-even, exp-odd	exp-odd, exp-odd
(b)	exp-even, exp-even	exp-odd, exp-odd	exp-even, exp-odd	exp-odd, exp-even
(c)	exp-odd, exp-even	exp-odd, exp-odd	exp-even, exp-odd	exp-even, exp-even
(d)	exp-odd, exp-odd	exp-odd, exp-even	exp-even, exp-odd	exp-even, exp-even
(e)	exp-odd, exp-odd	exp-even, exp-even	exp-even, exp-odd	exp-odd, exp-even
(f)	exp-odd, exp-even	exp-even, exp-even	exp-even, exp-odd	exp-odd, exp-odd

In each S, T combination, there are six even exponent entries, which together with $1 = v^0$ gives seven even exponents. Because the relations are

symbolic, we may choose any of the four combinations of S, T. She chooses S, T both even and using the relation $1 + v^T \equiv v^S \bmod q$, applies it to the sum of all the even terms, which we have required to be distinct. These sum to zero modulo q from the above result, so we have

$$1 + v^T + v^S + v^{2N-S} + v^{2N-T} + v^{S-T} + v^{T-S} \equiv 0 \bmod q.$$

Multiplying by v^{S+T} gives

$$v^{S+T} + v^{2T+S} + v^{2S+T} + v^T + v^S + v^{2T+S} \equiv 0 \bmod q,$$

which factorizes to give $(1+v^T)v^S(1+v^S+v^T) \equiv 0 \bmod q \equiv 2v^S v^S v^S \bmod q$ since $1 + v^T \equiv v^S \bmod q$. Since 2 is not a pth power, but the other terms are, this cannot occur, so the terms cannot all be distinct.

She next examines the case where one of the right hand side powers of v equals one of the left hand side powers of v, and apply the same techniques as above. Firstly for the list (a1) to (f1) from the previous section:

(a1) $1 + v^{2N-S} \equiv v^S \bmod q$, (b1) $1 + v^S \equiv v^{2S} \bmod q$,
(c1) $1 + v^{N-S} \equiv v^{2N-2S} \bmod q$, (d1) $1 + v^{N+S} \equiv v^{N-S} \bmod q$,
(e1) $1 + v^{N+2S} \equiv v^{N+S} \bmod q$, (f1) $1 + v^{N-2S} \equiv v^{2N-S} \bmod q$.

We construct a summary similar to that above, also including their x representation derived in the previous section:

	S even	S odd	x representation
(a1)	exp-even, exp-even	exp-odd, exp-odd	$-(x+2)$, $-(x+1)$
(b1)	exp-even, exp-even	exp-odd, exp-even	$-(x+1)$, $-x$
(c1)	exp-odd, exp-even	exp-even, exp-even	$x+2$, $x+3$
(d1)	exp-odd, exp-odd	exp-even, exp-even	$x+1$, $x+2$
(e1)	exp-odd, exp-odd	exp-odd, exp-even	x, $x+1$
(f1)	exp-odd, exp-even	exp-odd, exp-odd	$-(x+3)$, $-(x+2)$

For the list (a2) to (f2) we have:

(a2) $1 + v^{N+2S} \equiv v^S \bmod q$, (b2) $1 + v^{N-2S} \equiv v^{N-S} \bmod q$,
(c2) $1 + v^{N-S} \equiv v^{N+S} \bmod q$, (d2) $1 + v^{N+S} \equiv v^{2S} \bmod q$,
(e2) $1 + v^{2N-S} \equiv v^{2N-2S} \bmod q$, (f2) $1 + v^S \equiv v^{2N-S} \bmod q$.

with the following summary table.

	S even	S odd	x representation
(a1)	exp-odd, exp-even	exp-odd, exp-odd	$-(x+3)$, $-(x+2)$
(b2)	exp-odd, exp-odd	exp-odd, exp-even	x, $x+1$
(c2)	exp-odd, exp-odd	exp-even, exp-even	$x+1$, $x+2$
(d2)	exp-odd, exp-even	exp-even, exp-even	$x+2$, $x+3$
(e2)	exp-even, exp-even	exp-odd, exp-even	$-(x+1)$, $-x$
(f2)	exp-even, exp-even	exp-odd, exp-odd	$-(x+2)$, $-(x+1)$

By inspection x, $x+1$, $x+2$ are all exp-odd or all exp-even in either table. If they are exp-even, we define $w \equiv x+1 \equiv u^2 \bmod q$, where u is some pth power. This gives $w^6+w^5+w^4+w^3+w^2+w+1 \equiv 0 \bmod q$, regardless of whether or not w is a primitive Nth root of 1 modulo q, as the analysis at the start of this section shows.

Now $w^2+w \equiv x^2+2x+1+x+1 \equiv (x+1)(x+2) \equiv 1 \bmod q$ (recall the last equivalence from the previous section). We can apply this repeatedly: $2w^4+w^3+w^2+w+1 \equiv 0 \bmod q$; $-w^3+3w^2+w+1 \equiv 0 \bmod q$; $w^3+w^2-w \equiv 0 \bmod q$; $4w^2+1 \equiv 0 \bmod q$.

If $x, x+1, x+2$ are all exp-odd, $-(x+2)$ is exp-even by inspection. Defining $z \equiv -(x+2) \equiv u^2 \bmod q$, where u is some pth power, we have

$$z^6+z^5+z^4+z^3+z^2+z+1 \;\equiv\; 0 \bmod q.$$

Let $w = x+2 = -z$. Then $w^6-w^5+w^4-w^3+w^2-w+1 \equiv 0 \bmod q$. Now

$$w^2-w \;=\; x^2+4x+4-x-2 \;=\; (x+1)(x+2) \;\equiv\; 1 \bmod q,$$

which we can apply repeatedly: $2w^4-w^3+w^2-w+1 \equiv 0 \bmod q$; $w^3+3w^2-w+1 \equiv 0 \bmod q$; $w^3-w^2-w \equiv 0 \bmod q$; $4w^2+1 \equiv 0 \bmod q$

So whether or not $x+1$ is exp-even or exp-odd, we get $4w^2 \equiv -1 \bmod q$ for some pth power w. We have already ruled out 2 as a pth power, so 4 must be a pth power which is also an odd power of w, since w^2 is an even power, and $-1 \equiv w^N \bmod q$ is an odd power.

Since $w^{2N} \equiv 1 \bmod q$, we just need to check the factors of

$$4^{14}-1 \;=\; 5 \times 3 \times (14 \times 2+1)(14 \times 8+1)(14 \times 3+1)(14 \times 9+1).$$

Since p must be a prime, we need to examine $p=2$, $q=29$ and $p=3$, $q=43$. We have $32^3 \equiv 2 \bmod 43$, so $p=3, q=43$ is excluded. This exclusion of $p=3$ was also predicted from the table on page 2. The squares modulo 29, sorted into order, are 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28, and we have 4, 5, 6, 7 and -7, -6, -5, -4 as the eight consecutive entries predicted. We have therefore proved case 1 of Fermat's Last Theorem for (at least) $p = 47, 59, 167$.

Interestingly, Legendre recognizes the case of $p=3$, $q=43$ arising from $v^j \equiv \pm 2 \bmod q$, with $0 < j < 7$, and it happens that 32 is a primitive 14th root modulo 43. He defines his way round this by only considering $p > 3$, rather than introducing the condition $n^p \not\equiv 2 \bmod q$ (see Ribenboim (1991), section IV.1 1E case 5, pp. 116–117).

Sophie Germain's proof for $N = 8$

Note that the introductory part of the summary of the proof in Del Centina (2008) p. 369 is wrong: 'Let $P = 16p + 1$. We already know that there are no pairs of consecutive residues for primes of the form $8p + 1$, therefore two even integers t, s do not exist such that $1 + rt \equiv rs \bmod P$'. This conclusion comes from a different argument given below, but not spelt out in the manuscript.

Since $N = 8$ is even the lists (a) to (f), (a1) to (f1), and (a2) to (f2) are different from those for $N = 7$:
Recall that list (a) to (f) applies when all the powers of v are distinct.

	S even, T even	S even, T odd	S odd, T even	S odd, T odd
(a)	exp-even, exp-even	exp-odd, exp-even	exp-even, exp-odd	exp-odd, exp-odd
(b)	exp-even, exp-even	exp-odd, exp-odd	exp-even, exp-odd	exp-odd, exp-even
(c)	exp-even, exp-even	exp-even, exp-odd	exp-odd, exp-odd	exp-odd, exp-even
(d)	exp-even, exp-even	exp-even, exp-odd	exp-odd, exp-even	exp-odd, exp-odd
(e)	exp-even, exp-even	exp-odd, exp-odd	exp-odd, exp-even	exp-even, exp-odd
(f)	exp-even, exp-even	exp-odd, exp-even	exp-odd, exp-odd	exp-even, exp-odd

Since $N = 8$, we must have eight exp-even and eight exp-odd entries. For S, T both even, we have twelve exp-even entries, and for all other cases, we have eight exp-odd entries, which together with -1 would make nine, so in all cases, the entries cannot all be distinct. Recall that lists (a1) to (f1), and (a2) to (f2) apply when a left hand side power of v equals one on the right hand side:

(a1) $1 + v^{2N-S} \equiv v^S \bmod q$, (b1) $1 + v^S \equiv v^{2S} \bmod q$,
(c1) $1 + v^{N-S} \equiv v^{2N-2S} \bmod q$, (d1) $1 + v^{N+S} \equiv v^{N-S} \bmod q$,
(e1) $1 + v^{N+2S} \equiv v^{N+S} \bmod q$, (f1) $1 + v^{N-2S} \equiv v^{2N-S} \bmod q$.

The summary table is as follows.

	S even	S odd	x representation
(a1)	exp-even, exp-even	exp-odd, exp-odd	$-(x+2)$, $-(x+1)$
(b1)	exp-even, exp-even	exp-odd, exp-even	$-(x+1)$, $-x$
(c1)	exp-even, exp-even	exp-odd, exp-even	$x+2$, $x+3$
(d1)	exp-even, exp-even	exp-odd, exp-odd	$x+1$, $x+2$
(e1)	exp-even, exp-even	exp-even, exp-odd	x, $x+1$
(f1)	exp-even, exp-even	exp-even, exp-odd	$-(x+3)$, $-(x+2)$

For the list (a2) to (f2) we have:

(a2) $1 + v^{N+2S} \equiv v^S \bmod q$, (b2) $1 + v^{N-2S} \equiv v^{N-S} \bmod q$,
(c2) $1 + v^{N-S} \equiv v^{N+S} \bmod q$, (d2) $1 + v^{N+S} \equiv v^{2S} \bmod q$,
(e2) $1 + v^{2N-S} \equiv v^{2N-2S} \bmod q$, (f2) $1 + v^S \equiv v^{2N-S} \bmod q$.

with the following summary table.

	S even	S odd	x representation
(a1)	exp-even, exp-even	exp-even, exp-odd	$-(x+3)$, $-(x+2)$
(b2)	exp-even, exp-even	exp-even, exp-odd	x, $x+1$
(c2)	exp-even, exp-even	exp-odd, exp-odd	$x+1$, $x+2$
(d2)	exp-even, exp-even	exp-odd, exp-even	$x+2$, $x+3$
(e2)	exp-even, exp-even	exp-odd, exp-even	$-(x+1)$, $-x$
(f2)	exp-even, exp-even	exp-odd, exp-odd	$-(x+2)$, $-(x+1)$

This time, we only have eight distinct entries. For S even, we still have too many, since 1 is an exp-even, so we need to consider the case where S is odd, where we have four exp-odd and four exp-even entries. From previous analysis, we have$(x+1)(x+2) \equiv 1 \bmod q$, giving $x^2+3x+1 \equiv 1 \bmod q$, whence $x^4 \equiv 9x^2+6x+1 \bmod q$ and $(x+1)^2 \equiv -x \bmod q$.

In both cases, x is exp-even $= v^{2a}$ say, and $v^{2N} \equiv 1 \bmod q$, so $x^N = x^8 \equiv 1 \bmod q$. In the case $x^4 \equiv 1 \bmod q$, we have $x^4 \equiv 1 \equiv 9x^2+6x+1$, so $3x(x+2) \equiv 0 \bmod q$. By stipulation q is not a multiple of 3, and $x \not\equiv 0 \bmod q$, so $3x+2 \equiv 0 \bmod q$. But $-(3x+1) \equiv x^2 \bmod q$, so adding, we get $x^2 \equiv 1 \bmod q$, impossible. In the case $x^4 \equiv -1 \bmod q$, we have $x^4 \equiv -1 \equiv 9x^2+6x+1$, so

$$9x^2+6x+2 \;\equiv\; 0 \;\equiv\; 9x^2-2x^2 \;\equiv\; 7x^2 \mod q,$$

using $-(3x+1) \equiv x^2 \bmod q$ again. Since q is prime, and of the form $16p+1$, we get $x^2 \equiv 0 \bmod q$, impossible.

We have therefore proved case 1 of Fermat's Last Theorem for (at least) $p = 61$. While it is clear she is trying to invent an inductive method for tackling $N = 10$ and beyond, this is very much 'work in progress', so is not pursued further here.

References

Del Centina, A. (2008), 'Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's Last Theorem', *Archive for History of Exact Sciences* Vol. 62 No. 4, 349–392.

Edwards, H. M. (1977), *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, New York, Springer.

Laubenbacher, R. and Pengelley, D. (2010), 'Voici ce que j'ai trouvé: Sophie Germain's grand plan to prove Fermat's Last Theorem', *Historia Mathematica* Vol. 37 Issue 4, 641–692.

Ribenboim, P. (1991), *Fermat's Last Theorem for Amateurs*, New York, Springer.

Solution 235.4 – Matrix

Construct an $n \times n$ matrix as follows. Partition n into n_1 and n_2, $n_1, n_2 \geq 2$, and divide the matrix into four parts. The top left part is an $n_1 \times n_1$ matrix with a on the diagonal and c everywhere else. The bottom right part is an $n_2 \times n_2$ matrix with b on the diagonal and d everywhere else. The rest of the matrix elements are e. Also we insist that a, b, c, d and e are integers satisfying $a \neq b$, $a \neq c$ and $b \neq d$.

In every example I (TF) have created I have observed that the rank of the matrix is either n or $n-1$. So here is the problem: Either prove that the matrix has rank at least $n-1$, or find a counter-example. Also it would be nice to know exactly when rank $n-1$ occurs.

Dave Wild

The rank of a matrix can be determined by finding the number of linearly independent rows of the matrix. Adding two columns which contain zeros to the end of each row gives another matrix with the same rank. Add row $n+1$, which contains c in the first n_1 columns, e in the next n_2 columns, and 0 and 1 in the last two columns. Add row $n+2$, which contains e in the first n_1 columns, d in the next n_2 columns, and 1 and 0 in the last two columns. As these additional rows are linearly independent of all the other rows in the matrix it follows that the new $(n+2) \times (n+2)$ matrix has a rank 2 more than the original matrix. Now subtract row $n+1$ from the first n_1 rows and row $n+2$ from the following n_2 rows.

For example, when $n_1 = 3$ and $n_2 = 4$ the initial and resultant $(n+2) \times (n+2)$ matrices are

$$\begin{bmatrix} a & c & c & e & e & e & e & 0 & 0 \\ c & a & c & e & e & e & e & 0 & 0 \\ c & c & a & e & e & e & e & 0 & 0 \\ e & e & e & b & d & d & d & 0 & 0 \\ e & e & e & d & b & d & d & 0 & 0 \\ e & e & e & d & d & b & d & 0 & 0 \\ e & e & e & d & d & d & b & 0 & 0 \\ c & c & c & e & e & e & e & 0 & 1 \\ e & e & e & d & d & d & d & 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} f & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & f & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & f & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & g & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & g & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & g & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & g & -1 & 0 \\ c & c & c & e & e & e & e & 0 & 1 \\ e & e & e & d & d & d & d & 1 & 0 \end{bmatrix},$$

where $f = a - c$ and $g = b - d$.

As $a \neq c$ and $b \neq d$, both f and g are non-zero. Therefore the first n rows are linearly independent and the rank of the $(n+2) \times (n+2)$ matrix is at least n. From row $n+1$ subtract c/f times the first n_1 rows and e/g times the following n_2 rows so that the first n columns of this row are zero. From row $n+2$ subtract e/f times the first n_1 rows and d/g times the following n_2 rows so the first n columns of this row are also zero. The bottom right hand corner of the matrix becomes

$$\begin{bmatrix} \dfrac{n_2 e}{g} & 1+\dfrac{n_1 c}{f} \\ 1+\dfrac{n_2 d}{g} & \dfrac{n_1 e}{f} \end{bmatrix} = \begin{bmatrix} \dfrac{n_2 e}{b-d} & 1+\dfrac{n_1 c}{a-c} \\ 1+\dfrac{n_2 d}{b-d} & \dfrac{n_1 e}{a-c} \end{bmatrix}$$

$$= \begin{bmatrix} \dfrac{n_2 e}{b-d} & \dfrac{a+(n_1-1)c}{a-c} \\ \dfrac{b+(n_2-1)d}{b-d} & \dfrac{n_1 e}{a-c} \end{bmatrix}.$$

If all of these elements are zero then the original matrix has rank $n-2$. This occurs when

$$e \;=\; a+(n_1-1)c \;=\; b+(n_2-1)d \;=\; 0.$$

If not all the elements are zero but the determinant of the 2×2 matrix is zero then the rank of the original matrix will be $n-1$. This occurs when

$$n_1\, n_2\, e^2 \;=\; (a+(n_1-1)c)\,(b+(n_2-1)d)\,.$$

In other cases the rank of the original matrix is n. These criteria agree with the examples of matrices given in the problem.

Problem 273.1 – Hair

When you visit your hairdresser within 30 days of your previous appointment the cost is £30. Thereafter she adds a premium of $30\,d^{5/4}$ pence, where d is the number of further days you delay your next appointment. For example, if you leave it for 42 days, the cost will be £36.70035…, which we assume she will round to £36.70. Obviously, in her view the surcharge is justified as compensation for additional work created by excessive hair growth.

If you get your hair cut at regular finite intervals to maintain a neat and tidy appearance at minimum cost, how often should you go?

Cattle

Tony Forbes

Farm animals have often featured significantly in M500—as one can see by looking at past issues. But recently, perhaps inspired by an episode of *The Archers*, I became interested in that most famous cow conundrum of ancient times, ***Archimedes' Cattle Problem***. A brief search on the Web failed to produce a complete solution that I could readily understand; so I decided to work it out for myself. And having done so I feel obliged to share the results of my labours with readers of this magazine.

According to *Recreations in the Theory of Numbers* by Albert Beiler, Archimedes begins (in English), *'Compute, O friend, the host of the cattle of the Sun, giving thy mind thereto, if thou hast a share of wisdom. Compute the number which once grazed on the fields of the Thrinacian isle of Sicily, ...'* In modern terminology he asks for (presumably the smallest) positive integers W, X, Y, Z, w, x, y, z that satisfy

$$\begin{aligned} W &= \left(\frac{1}{2}+\frac{1}{3}\right)X+Z, \quad X = \left(\frac{1}{4}+\frac{1}{5}\right)Y+Z,\\ Y &= \left(\frac{1}{6}+\frac{1}{7}\right)W+Z,\\ w &= \left(\frac{1}{3}+\frac{1}{4}\right)(X+x), \quad x = \left(\frac{1}{4}+\frac{1}{5}\right)(Y+y),\\ y &= \left(\frac{1}{5}+\frac{1}{6}\right)(Z+z), \quad z = \left(\frac{1}{6}+\frac{1}{7}\right)(W+w), \end{aligned}$$

$W+X$ is a square and $Y+Z$ is a triangular number.

The variables are actually the sizes of eight herds of cattle. Upper and lower case letters represent bulls and cows respectively, and these are further divided into four colours: W, w white, X, x black, Y, y dappled, Z, z yellow. However, these details need not concern us, and anyway, once you see the numbers it will be obvious that the herds must be imaginary. Otherwise the animals would have been very small.

The first seven equations form a linear system, which is solved to give

$$\begin{aligned} W &= \frac{3455494\,z}{1813071}, \quad X = \frac{828946\,z}{604357}, \quad Y = \frac{7358060\,z}{5439213}, \quad Z = \frac{461043\,z}{604357},\\ w &= \frac{2402120\,z}{1813071}, \quad x = \frac{543694\,z}{604357}, \quad y = \frac{1171940\,z}{1813071}, \end{aligned}$$

and we put $z = 5439213\,s$ to clear the denominators:

$$W = 10366482\,s,\quad X = 7460514\,s,\quad Y = 7358060\,s,\quad Z = 4149387\,s,$$
$$w = 7206360\,s,\quad x = 4893246\,s,\quad y = 3515820\,s,\quad z = 5439213\,s.$$

Of anyone who gets this far Archimedes says, *'If thou canst give, O friend, the number of bulls and cows in each herd, thou art not unknowing nor unskilled in numbers, but still not yet to be counted among the wise.'*

To comply with the eighth condition, $W + X = 17826996\,s$ is a square, all we need to do is replace s by $17826996/4\,t^2 = 4456749\,t^2$:

$$W = 46200808287018\,t^2,\quad X = 33249638308986\,t^2,$$
$$Y = 32793026546940\,t^2,\quad Z = 18492776362863\,t^2,$$
$$w = 32116937723640\,t^2,\quad x = 21807969217254\,t^2,$$
$$y = 15669127269180\,t^2,\quad z = 24241207098537\,t^2.$$

Well, that's the easy stuff out of the way—and already the herds are beginning to get quite large, even when $t = 1$. But if you wish to be counted among the wise and to *'go forth as conqueror, and rest assured that thou art proved most skilled in the science of numbers,'* it is necessary to deal with the last condition, which says that

$$Y + Z = 51285802909803\,t^2 = \frac{n(n+1)}{2}$$

for some positive integer n, or, after multiplying by 8 and adding 1,

$$8(Y + Z) + 1 = 4729494 \cdot (9314\,t)^2 + 1 = (2n+1)^2. \tag{1}$$

If we put $u = 2n + 1$ and $v = 9314\,t$, then (1) becomes

$$u^2 - 4729494\,v^2 = 1. \tag{2}$$

The procedure for solving equations like (2) is well known. Ignoring $(u, v) = (1, 0)$, we want the smallest positive solution (u_0, v_0), and we obtain it by computing (with a little help from MATHEMATICA) convergents u/v of the continued fraction for $\sqrt{4729494}$ until we find one which works. We succeed with

$$\sqrt{4729494} \approx [2174; 1, 2, 1, 5, 2, 25, 3, 1, 1, 1, 1, 1, 1, 15, 1, 2, 16, 1, 2, 1, 1, 8, 6,$$
$$1, 21, 1, 1, 3, 1, 1, 1, 2, 2, 6, 1, 1, 5, 1, 17, 1, 1, 47, 3, 1, 1, 6, 1, 1,$$
$$3, 47, 1, 1, 17, 1, 5, 1, 1, 6, 2, 2, 1, 1, 1, 3, 1, 1, 21, 1, 6, 8, 1, 1, 2,$$
$$1, 16, 2, 1, 15, 1, 1, 1, 1, 1, 1, 3, 25, 2, 5, 1, 2, 1],$$

and this gives the convergent u_0/v_0, where

$$\begin{aligned} u_0 &= 109931986732829734979866232821433543901088049, \\ v_0 &= 505494852343150330744778197355404089863 40. \end{aligned}$$

However, we are not done yet because, although $(u, v) = (u_0, v_0)$ satisfies (2), we have agreed that v must also be a multiple of 9314. So from (u_0, v_0) we generate further solutions of (2) by computing

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} u_0 & 4729494\, v_0 \\ v_0 & u_0 \end{bmatrix}^j \begin{bmatrix} u_0 \\ v_0 \end{bmatrix}, \qquad j = 1,\ 2,\ \ldots,$$

until we find one where 9314 divides v. We succeed when $j = 2328$. Then

$$\begin{aligned} u &= 37653445023472058840\ldots84777023371728320049 \quad (103273 \text{ digits}), \\ v &= 17313998589517710564\ldots02891212883491745860 \quad (103270 \text{ digits}), \end{aligned}$$

where for brevity we have omitted some of the digits. Observe that u is odd and you can take my word for it that $t = v/9314$ is an integer. Thus we have the smallest solution to Archimedes' problem:

$$\begin{aligned} t^2 &= 34555906354559370506\ldots82492556252058980100 \quad (206531 \text{ digits}), \\ W &= 15965108046711445314\ldots25054629385150341800 \quad (206545 \text{ digits}), \\ X &= 11489713877282899997\ldots42829072899825178600 \quad (206545 \text{ digits}), \\ Y &= 11331927544386380771\ldots11404453921175894000 \quad (206545 \text{ digits}), \\ Z &= 63903464823090286500\ldots22697068635296026300 \quad (206544 \text{ digits}), \\ w &= 11098298923733190397\ldots47790395914059564000 \quad (206545 \text{ digits}), \\ x &= 75359414205454263981\ldots96240177238562645400 \quad (206544 \text{ digits}), \\ y &= 54146089457145667802\ldots02462606608963318000 \quad (206544 \text{ digits}), \\ z &= 83767688241852443869\ldots74928222116422113700 \quad (206544 \text{ digits}), \\ \text{total}: &\ 77602714064868182695\ldots23406626719455081800 \quad (206545 \text{ digits}). \end{aligned}$$

Curiously, if we interchange squareness and triangularity in the last two conditions—that is, make $W + X$ a triangular number and $Y + Z$ a square—the solution is very similar. This time we put $s = 11507447\, t^2$ and we end up solving $4729494\,(2 \cdot 9314t)^2 + 1 = (2n+1)^2$, which also leads to equation (2). Moreover, the same v applies and we obtain the same numbers as before but multiplied by $11507447/17826996 = 2471/3828$. The new total will be

$$50093079011047356175\ldots35459188773190571350 \quad (206545 \text{ digits}).$$

Problem 273.2 – Square, split and add

Tony Forbes

Let b and d be integers greater than 1. Let n be an integer such that

$$b^{d-1} \;\le\; n \;\le\; b^d - 1 \quad \text{and} \quad \left\lfloor \frac{n^2}{b^d} \right\rfloor + (n^2 \bmod b^d) \;=\; n. \qquad (1)$$

Here is what we are really doing: take a d-digit number n in base b, square it, split n^2 into two numbers at the dth digit from the right and add the two parts. We get excited if n is unchanged by this process. Some examples will make things clear(er), and you can verify that the tabulated numbers really do have have the stated property. For instance, $703 = 494+209 = \sqrt{494209}$. When $b = 10$ they are known as *Kaprekar numbers*.

$b = 2$	3	7	10	15	31	36	63	127	136	171
3	8	13	14	26	65	80	121	122	242	273
4	6	10	15	28	36	63	85	120	136	171
5	9	16	24	32	93	124	144	208	273	352
6	15	21	35	86	130	215	260	371	630	666
7	16	33	48	153	171	172	190	324	342	576
8	28	36	63	147	365	511	820	910	1170	1261
9	16	65	80	105	169	273	456	560	624	728
10	45	55	99	297	703	999	2223	2728	4950	5050
11	16	25	40	81	96	105	120	190	210	266
12	66	78	143	628	1100	1727	2146	2640	3510	4785
13	49	57	64	105	112	120	168	244	549	793
14	40	66	91	105	130	156	195	845	1899	2743
15	64	161	224	483	1205	1687	1688	2170	2892	3374
16	51	85	120	136	171	205	255	351	820	910

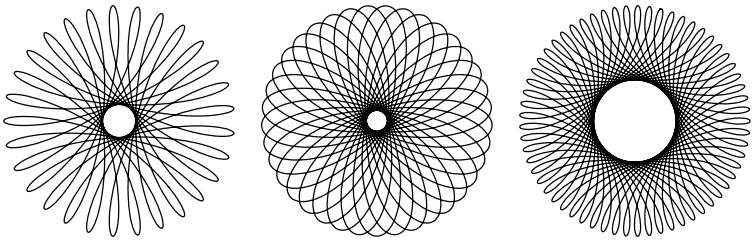
There are five primes in the table, namely 3, 7, 31, 127 and 13, and, remarkably, when they are represented in the relevant bases they look like this: 11_2, 111_2, 11111_2, 1111111_2 and 111_3 respectively. If you are prepared to extend the table a little (actually quite a lot) further, you will find more primes with a similar structure; for example, $305175781 = 1111111111111_5$, $16148168401 = 1111111111111_7$, $11111111111111111111_{10}$ and the same pattern in base 19 (this is a coincidence, surely), $109912203092239643840221 = 11111111111111111111_{19}$.

So here is the problem. Show that if n is a prime satisfying (1) for some integer $b > 1$, then $n = 111\ldots111_b$. Or find a counter-example.

Solution 271.1 – Complex exponential sums

Consider the functions

$$f(t) = \frac{1}{2}e^{-18it} - \frac{2i}{3}e^{11it}, \qquad g(t) = ie^{23it} - \frac{5}{6}e^{-14it},$$
$$\text{and} \qquad h(t) = \left(\frac{1}{3} + i\right)e^{-17it} + \frac{i}{2}e^{44it}.$$



Show that the graphs of $f(t)$, $g(t)$ and $h(t)$ have 29-fold, 37-fold and 61-fold rotational symmetry respectively.

Dick Boardman

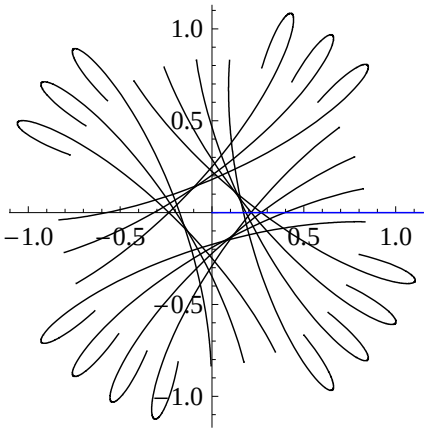
We have

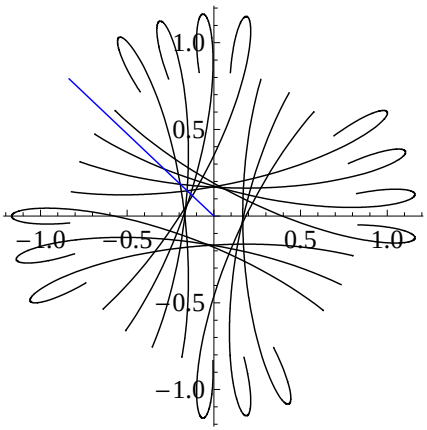
$$\begin{aligned} f\left(t + \frac{2\pi}{29}\right) &= \frac{1}{2}e^{-18it-36\pi i/29} - \frac{2i}{3}e^{11it+22\pi i/29} \\ &= e^{22\pi i/29}\left(\frac{1}{2}e^{-18it-36\pi i/29-22\pi i/29} - \frac{2i}{3}e^{11it}\right) \\ &= e^{-36\pi i/29}f(t). \end{aligned}$$

This relation shows that for all points t, the ratio $f(t + 2\pi/29)/f(t)$ is a constant complex number. Moreover, the constant has absolute value 1 and represents a rotation by an angle of $22\pi/29$ (approximately 136.55 degrees), producing the 29-fold symmetry. This is illustrated on the next page. Here we have split the graph of $f(t)$, $0 \le t < 2\pi$, into two parts: t in the even intervals $[2\pi j/29, 2\pi(j+1)/29)$, $j = 0, 2, 4, \ldots, 26$, left, and t in the odd intervals $[2\pi j/29, 2\pi(j+1)/29)$, $j = 1, 3, \ldots, 27$, right. Evidently the right-hand graph is obtained by rotating the left-hand graph by about 136.55 degrees.

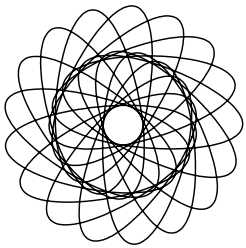
Similarly,

$$g\left(t + \frac{2\pi}{37}\right) = e^{-28\pi i/37}g(t) \quad \text{and} \quad h\left(t + \frac{2\pi}{61}\right) = e^{-34\pi i/61}h(t).$$

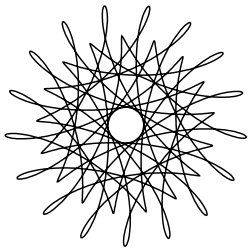




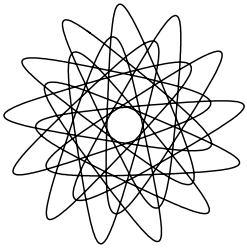
With three terms in the sum we can construct more complicated shapes.



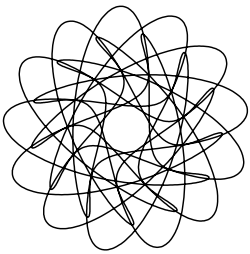
$$e^{15it} - \frac{i}{2}e^{-2it} + \frac{i}{3}e^{-19it}$$



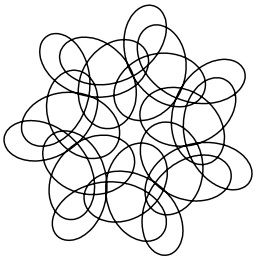
$$\frac{i}{3}e^{-6it} - e^{11it} - \frac{i}{2}e^{-23it}$$



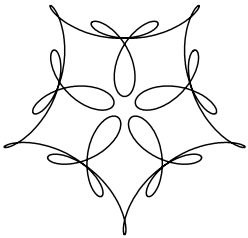
$$\frac{i}{3}e^{2it} + ie^{-11it} - \frac{1}{2}e^{15it}$$



$$\frac{i}{3}e^{23it} - ie^{10it} - \frac{1}{2}e^{-16it}$$



$$e^{it} + \frac{i}{3}e^{8it} + \left(\frac{1}{2} + \frac{i}{5}\right)e^{-20it}$$



$$e^{it} + \frac{i}{2}e^{6it} + \frac{i}{3}e^{-14it}$$

Referendum pie

Mike Grannell

It was 2025 when the trouble really began. There had been some muttering prior to this, but in July 2025, Microsoft introduced Windows 25. Every time users of OFFICE-INFINITY entered the consecutive characters pi, the system automatically started to produce the decimal digits of π to unlimited accuracy. Previous versions had a similar bug, but this could be turned off with a simple expletive to the voice-recognition system. Windows 25 was different—it had a mind of its own and would shout back in highly offensive terms.

At this point, demand began to grow for a referendum on the true value of π. Older people seemed to prefer $22/7$, but there were vigorous arguments in support of alternative values. The *Sun* newspaper was strongly in favour of taking the value to be 3 on grounds of simplicity, and it didn't care for the symbol π either, decrying it to be a foreign import. The *Daily Mail* and the *Daily Express* felt that their readers had had enough of so-called experts, particularly mathematicians and the like. Many of these people, it was alleged, were wasting a fortune computing π to billions of decimal places—in fact over 350 million digits per week on some reckoning. Overseas mathematicians were especially vilified as corrupting the innate simplicity of the English character by their slavish addiction to spurious accuracy. The public were informed that many foreign symbols had been imported into mathematics and the expense of dealing with these became a key issue. The president of the London Mathematical Society inadvertently let slip that many numbers in common use were irrational, and some even transcendental! Papers were uncovered relating to surreal numbers and even to imaginary numbers. The prime minister eventually conceded that a referendum would be held on 14th March 2026.

A close colleague of the London Mathematical Society president, a person with ambition for this post, suddenly switched sides and wrote extensive articles to the effect that a few decimal places would suffice, including one for *The Times* entitled 'Cutting π down to size'. He confessed that he had secretly felt this way for years, but had been unwilling to offend his erstwhile friend. Televised debates followed between the 'Pi is finite' and the 'Hands off π' camps. Foreign mathematicians were aghast. The 'Pi is finite' camp vigorously pushed the concept of simplicity and promised to replace π by p (to be pronounced pee). They were challenged to specify how many decimal places they would use, but their answers were evasive and varied

considerably. It was also pointed out that although π was a foreign (Greek) letter, p itself was a Roman import. But none of this seemed to stick. The *Star* ran a leader with the headline 'Pee off pi'. The 'Hands off π' group promised catastrophic disaster if π were to be redefined. They were portrayed in most of the media as elitist snobs and know-alls. Probably this was not helped by articles in the *Guardian* with headlines such as 'Why π will affect future generations and why its redefinition will lead to untold economic disasters in the distant future'.

The result of the referendum was narrow but, nevertheless, there was a clear victory for the 'Pi is finite' campaign, now renamed the 'P is finite' group. Media pundits analysing the result opined that the great English public had finally taken revenge for the mathematics that they had been forced to endure at school. The president of the London Mathematical Society resigned and there was a considerable revolt at the Institute of Mathematics and its Applications, whose president was regarded as having been insufficiently supportive of the 'Hands off π' campaign. Some backtrackers demanded a second vote, while others reluctantly agreed to settle for 355/113.

By 2040 we still don't have a definitive value for π, or p as it is now called. However, it is now illegal hate-speech to claim that it has infinitely many decimal places. A popular choice is $p = 22/7$, and the 'P is finite' team are constantly assuring people that things like wheels not being completely circular are merely transitional problems. England was forced out of the World Cup in 2038 for using a ball judged insufficiently spherical, and was beaten in the Mathematical Olympiad by the Vatican City youth team. Most international scientific societies expelled the English representatives, although this was hailed as a triumph by the English press. The University Research Excellence Framework was revised to promote the National Excellence category above the International Excellence category.

Meanwhile, at Heysham nuclear power station, and unknown to everyone, the non-circular reactor containment vessel has just developed the tiniest of cracks.

It was the kind of night I had never known. This was night to the power of night to the power of night. This was night cubed.

— M. Haig, *The Humans*

Exercise for reader: What is the value of night?

The allure of magic squares

Eddie Kent

In M500 we frequently talk about magic squares. In fact I once offered a prize of $100 for a particular one, which no one has bothered to claim yet. However, here is an astonishing result I just read about. The smallest possible magic square of 7th powers (it is said) was recently (2013) constructed by Toshihiro Shirakawa. Its size is 144×144 and its magic sum is

$$3141592653589793238462643383279502884197169399375105$$

and these are the first 52 digits of π. Clearly this gives an elegant way of producing π on request, rather than having to learn all those tedious mnemonics; just knock up the correct magic square and read it off. Also of course this proves that π is not random at all but contains magical properties. Or might if it weren't that with a big enough 'magic' square you can stuff nearly anything into it with a bit of ingenuity. Look what Dürer did.

He keeps bob bob bobbin' along

Dave Wild

Oxford University Press have published over 200 books in a series of *Very Short Introductions* to a variety of subjects. A recent addition is one on Combinatorics by Robin Wilson, Emeritus Professor at the OU. It mentions that parts of the book follow the general approach of *TM361, Graphs, Networks and Design*, which ran from 1981 to 1994. If you look on Amazon then the table of contents and index will give you a good idea of the scope of the book.

I found the parts of the book I have read to be well written. In the chapter on Permutations and Combinations, 'Another important result Combination rule 2' was the same as Combination rule 1.

This proves the book was based on an OU course. Robin's *An Intoduction to Graph Theory* which was first published in 1972 reached its 5th edition in 2010. He is to be congratulated on its longevity.

Problem 273.3 – Rational integral

Show that

$$\int_0^{2\pi} \frac{(\cos x)\left(\sin \dfrac{x}{2}\right)}{\left(\cos \dfrac{x}{3}\right)\left(\sin \dfrac{x}{4}\right)}\, dx \;=\; -\frac{368}{55}.$$

Problem 273.4 – Sums of reciprocals of primes

It is clear (TF thinks) that a sum of reciprocals of distinct primes can never add up to 1. If not 1, what about something that is nearly 1? Can you find sets of distinct primes $\{p_1, p_2, \ldots, p_r\}$ such that

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r} = \frac{a \pm 1}{a}$$

for some integer a, as, for example, $1/2 + 1/3 + 1/7 = 41/42$? Are there infinitely many examples?

M500 Mathematics Revision Weekend 2017

The forty-third M500 Revision Weekend will be held at

Kents Hill Park Training and Conference Centre,
Milton Keynes, MK7 6BZ
from Friday 12th to Sunday 14th May 2017.

The standard cost, including accommodation (with en suite facilities) and all meals from dinner on Friday evening to lunch on Sunday is £285. The standard cost for non-residents, including Saturday and Sunday lunch, is £170. There will be an early booking period up to 11th April with a discount of £20 for both members and non-members.

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 2017 must be paid in full before the booking is confirmed. Members will be entitled to a discount of £15 for all applications.

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 at

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.

04.00

Problem 273.5 – Twisted prisms

The *edge chromatic number*, $\chi'(G)$, of a graph G is the minimum number of colours required to colour the edges of G such that any two edges meeting at a vertex have distinct colours.

Let $n \geq 3$ and $d < n/2$ be positive integers and construct a 3-regular graph $P_{n,d}$ as follows. There are $2n$ vertices, A_i and B_i, $i = 0, 1, \ldots, n-1$. The edges are $\{A_i, A_{i+1 \bmod n}\}$, $\{B_i, B_{i+d \bmod n}\}$ and $\{A_i, B_i\}$, $i = 0, 1, \ldots, n-1$. Some examples are on the front cover.

Show that $\chi'(P_{n,d}) = 3$, with precisely one exception: $n = 5$, $d = 2$, also known as the Petersen graph, where $\chi'(P_{5,2}) = 4$.

Front cover Twisted prisms