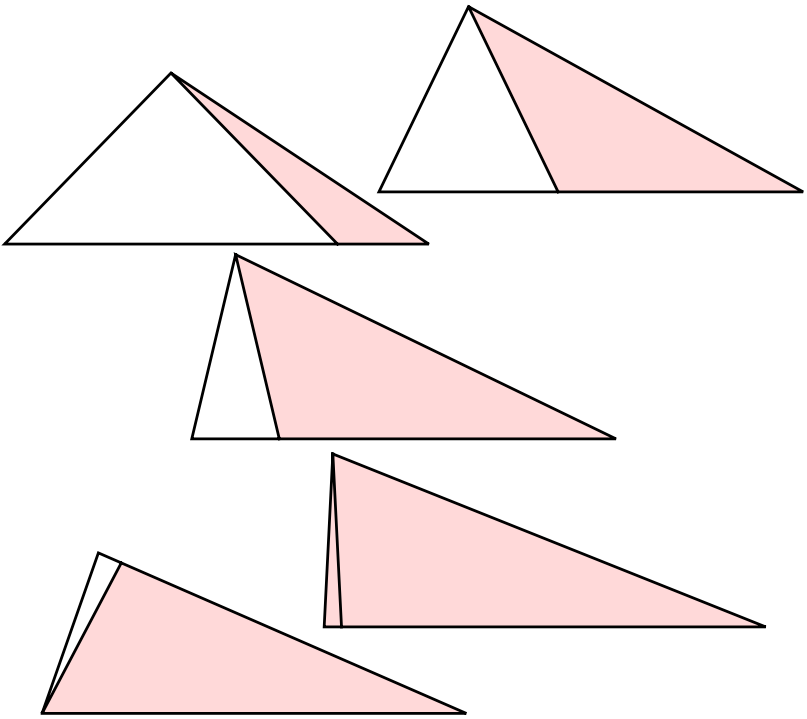
*

ISSN 1350-8539

M500

M500 272



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 full details and a booking form see m500.org.uk/may.

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

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

Multiple angle relationships in integer triangles

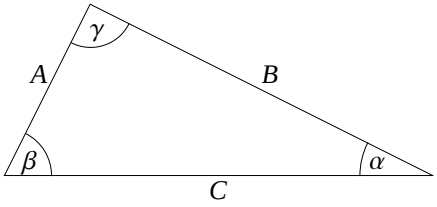
Chris Pile

Introduction

The $(3, 4, 5)$ triangle is a well-known scalene triangle with integer sides having one angle of $90°$. Other right-angled triangles can be created, also with integer sides, giving the set of (primitive) Pythagorean triples.

Considering other integer-sided triangles leads immediately to the $(4, 5, 6)$ triangle. Inspection shows that this triangle has one angle (the largest) exactly double the smallest angle.[1] It is interesting to see if other triangles have this property, or, more generally, with other angle multiples.

To list, order and compare triangles, it is convenient to specify them in lowest terms (primitives) and in order of side lengths.



Thus A, B, C is an integer-sided triangle such that $C > B > A$ and $\gcd(A, B, C) = 1$. Let the angles opposite the sides A, B, C be α, β, γ respectively.

Double angle

Three cases of double angles can occur.

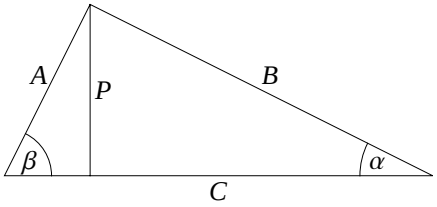
(i) $\beta = 2\alpha$. This implies $0 < \alpha < 36°$, $0 < \beta < 72°$, $180° > \gamma > 72°$. Note that if $\alpha > 30°$, then all angles are acute.

(ii) $\gamma = 2\alpha$. This implies $36° < \alpha < 45°$, $72° > \beta > 45°$, $72° < \gamma < 90°$. In this case all angles are acute.

(iii) $\gamma = 2\beta$. Here, $45° > \alpha > 0$, $45° < \beta < 60°$, $90° < \gamma < 120°$. In this case γ is always obtuse.

(i) $\beta = 2\alpha$

A modest computer search reveals the selection on the next page. Note that A is a square. Also $\cos\alpha$ is rational. Indeed,



$$\cos\alpha = \frac{C^2 + B^2 - A^2}{2CB}, \quad \sin\alpha = \frac{P}{B}, \quad \sin\beta = \frac{P}{A}.$$

[1] The editor of this magazine is astonished to learn that he has spent most of his life being unaware of this fact. — TF

A	B	C	α	β	$\cos\alpha$
9	15	16	33.5573	67.1146	5/6
16	28	33	28.955	57.91	7/8
25	45	56	25.8419	51.6839	9/10
36	66	85	23.5565	47.1129	11/12
49	84	95	31.0027	62.0054	6/7
49	91	120	21.7868	43.5736	13/14
64	104	105	35.6591	71.3182	13/16
64	120	161	20.3641	40.7283	15/16
81	144	175	27.266	54.5321	8/9
81	153	208	19.1881	38.3763	17/18
100	170	189	31.7883	63.5767	17/20
100	190	261	18.1949	36.3897	19/20

As $\beta = 2\alpha$, $\sin\beta = 2\sin\alpha\cos\alpha$. Hence

$$\frac{P}{A} \;=\; 2\,\frac{P}{B}\cdot\frac{C^2+B^2-A^2}{2CB}.$$

Therefore $CB^2 = AC^2 + AB^2 - A^3$, which implies

$$B^2(C-A) \;=\; A(C^2-A^2) \;=\; A(C-A)(C+A),$$

which leads to $B^2 = AC + A^2$, or $AC = B^2 - A^2$. Therefore

$$\cos\alpha \;=\; \frac{C^2+AC}{2BC} \;=\; \frac{A+C}{2B} \;=\; \frac{B}{2A}.$$

(ii) $\gamma = 2\alpha$

Triangles of this type may be less common because α is restricted to a small range. The $(4, 5, 6)$ triangle is one example, already mentioned. Other triangles were revealed by a computer search.

A	B	C	α	$\cos\alpha$
4	5	6	41.4096	3/4
25	39	40	36.8699	4/5
49	51	70	44.4153	5/7
49	72	77	38.2132	11/14
81	88	117	43.7617	13/18
81	115	126	38.9424	7/9

For this case, $AB = C^2 - A^2$ and $\cos\alpha = C/(2A)$. Again, side A is a square and $\cos\alpha$ is rational. Also $A < B < \phi A$, where $\phi = 1.618\ldots$ is the golden ratio.

(iii) $\gamma = 2\beta$

The range of γ is between 90° and 120°. In this case B is a square,

$$AB \;=\; C^2 - B^2 \quad \text{and} \quad \cos\beta \;=\; \frac{C}{2B}.$$

A	B	C	β	$\cos\beta$
7	9	12	48.1897	2/3
9	16	20	51.3178	5/8
11	25	30	53.1301	3/5
13	36	42	54.3147	7/12
15	49	56	55.1501	4/7
17	64	72	55.7711	9/16
19	81	90	56.251	5/9
21	100	110	56.633	11/20
23	121	132	56.9443	6/11
24	25	35	45.573	7/10
25	144	156	57.2028	13/24

A	B	C	β	$\cos\beta$
27	169	182	57.421	7/13
29	196	210	57.6076	15/28
32	49	63	49.9948	9/14
40	81	99	52.3301	11/18
48	121	143	53.7785	13/22
56	169	195	54.7656	15/26
57	64	88	46.5675	11/16
69	100	130	49.4584	13/20
75	121	154	50.4788	7/11
87	169	208	52.0201	8/13
93	196	238	52.6168	17/28

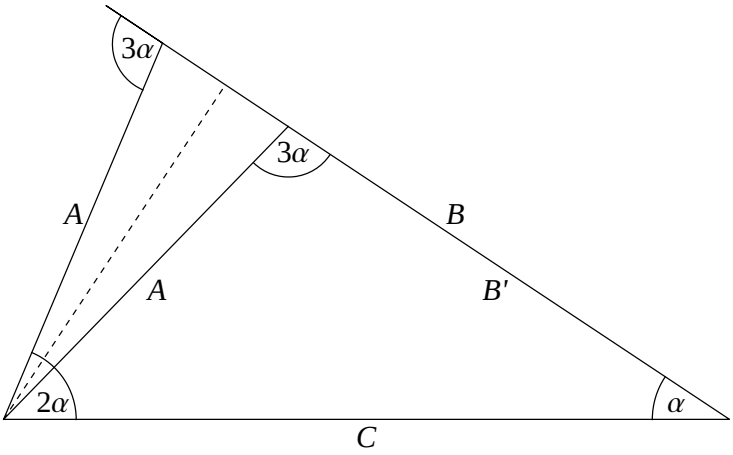
Triple angle

Again, three cases can occur.

(i) $\beta = 3\alpha$: $0 < \alpha \lessapprox 25.71°$, $0 < \beta \lessapprox 77.14°$, $180° > \gamma \gtrapprox 77.14°$.

(ii) $\gamma = 3\alpha$: $25.71° \lessapprox \alpha < 36°$, $77.14° \gtrapprox \beta > 36°$, $77.14° \lessapprox \gamma < 108°$.

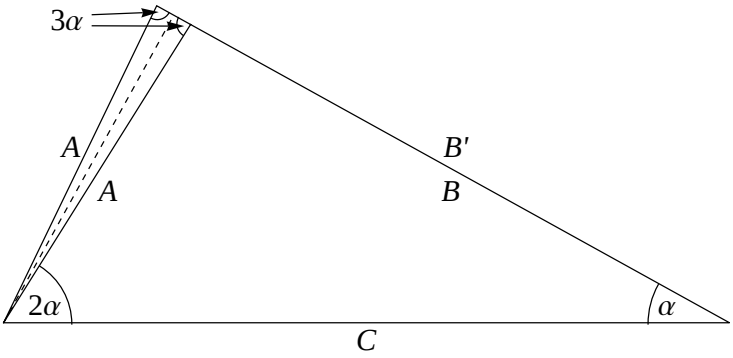
(iii) $\gamma = 3\beta$: $36° > \alpha > 0$, $36° < \beta < 45°$, $108° < \gamma < 135°$.



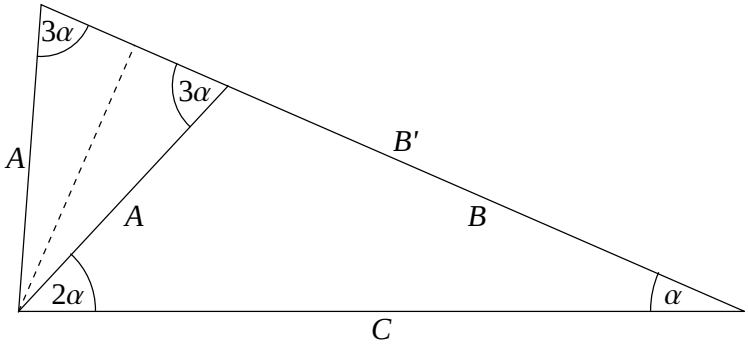
A triple-angle triangle can be constructed from a double-angle triangle as one external angle will be the triple.

From $\beta = 2\alpha$, $30° < \alpha < 36°$, as in the diagram at the bottom of the previous page, we have, for example, $(A, B, C) = (9, 15, 16)$ with $\alpha \approx 33.56$. The new triangle has $B' = 35/3$ or, in integers, $(A, B', C) = (27, 35, 48)$.

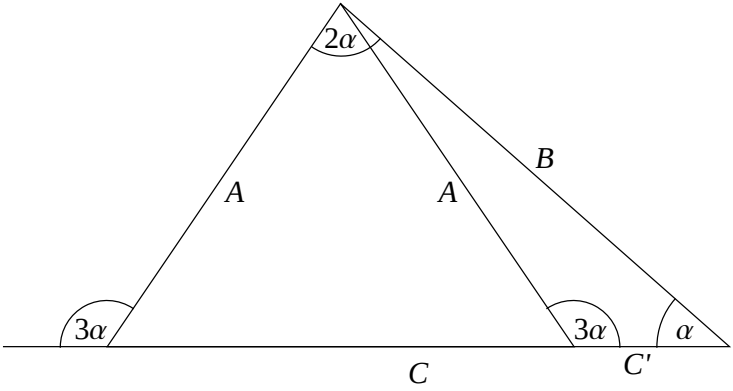
Using the following diagram, which applies when $25.71° \lessapprox \alpha < 30°$, we have, for example, $(A, B, C) = (16, 28, 33)$ with $\alpha \approx 28.96$. Then the new triangle has $B' = 119/4$ or, in integers, $(A, B', C) = (64, 119, 132)$. In each case the new side is still mid-length; so $\gamma = 3\alpha$.



When $0 < \alpha \lessapprox 25.71°$ we have, for example, $\alpha \approx 23.56°$ and $(A, B, C) = (36, 66, 85)$, as in the next diagram. Now B has to be extended by $143/6$, the new triangle being $(36, 539/6, 85)$ and so $B' > C$. After scaling to integers, rearranging and renaming the sides and angles, the triangle becomes $(A, B, C) = (216, 510, 539)$ with $\beta = 3\alpha$.



From $\gamma = 2\alpha$, we use $(A, B, C) = (4, 5, 6)$ with $\alpha \approx 41.41°$, as in the next diagram. In this case the new side is $C' = 3/2$, which becomes the smallest side: $(A, B, C') = (4, 5, 3/2)$. Rearranging, the new triangle in integers is $(3, 8, 10)$ and $\gamma = 3\beta$.



Quadruple angles

In a similar manner we can use a triple-angle triangle to construct one with a quadruple angle. In each of the following examples one side is a fourth power. [TF — To make your life a little more challenging and mine a lot easier, I decided not to reproduce every detail of the author's drawings. You should have no difficulty annotating the pictures on the front cover.]

From triangle $(A, B, C) = (27, 35, 48)$ with $\cos\alpha = 5/6$, $\alpha \approx 33.56°$, the external angle is 4α and $C' = 48 - 2 \cdot 113/6 = 31/3$. Therefore the new triangle is $(27, 35, 31/3)$ or, rearranging, $(31, 81, 105)$ with $\gamma = 4\beta$.

From triangle $(A, B, C) = (64, 119, 132)$ with $\cos\alpha = 7/8$, $\alpha \approx 28.955°$, the external angle is 4α and $C' = 132 - 2 \cdot 223/8 = 305/4$. Therefore the new triangle is $(64, 119, 305/4)$ or, rearranging, $(256, 305, 476)$ and $\gamma = 4\alpha$.

From triangle $(A, B, C) = (125, 279, 280)$ with $\cos\alpha = 9/10$, $\alpha \approx 25.84°$, $C' = 280 - 2 \cdot 289/10 = 1111/5$. The new triangle is $(125, 279, 1111/5)$ or, rearranging, $(625, 1111, 1395)$ with $\gamma = 4\alpha$.

From triangle $(A, B, C) = (216, 510, 539)$ with $\cos\alpha = 11/12$, $\alpha \approx 23.56°$, $B' = 510 - 2 \cdot 191/12 = 2869/6$. The new triangle is $(216, 2869/6, 539)$ or, rescaling, $(1296, 2869, 3234)$ and $\gamma = 4\alpha$.

From triangle $(A, B, C) = (343, 840, 923)$ with $\cos\alpha = 13/14$, $\alpha \approx 21.787°$, $B' = 840 + 2 \cdot 239/14 = 6119/7$. The new triangle is $(343, 6119/7, 923)$ or, rescaling, $(2401, 6119, 6461)$ with $\gamma = 4\alpha$.

Sophie Germain and Fermat's Last Theorem – I

Roger Thompson

Introduction

M500 **211** briefly mentions Sophie Germain and her contribution to Fermat's Last Theorem. This article goes into some of the mathematical details.

Sophie Germain (1776–1831) was perhaps the first world-class female mathematician. A summary of all her work and her life is given in

http://en.wikipedia.org/wiki/Sophie_Germain,

which also has many links to further reference material. Such status is all the more remarkable because she was self-taught—a consequence of women not being admitted to French universities. Although she was forced to correspond with the great mathematicians Lagrange and Gauss under the pseudonym Antoine-Auguste LeBlanc, it is heartening to note that when her true identity was revealed, both mathematicians continued to encourage her work. This situation has some similarities with that of a hundred years later, when G. H. Hardy recognised the genius of the self-taught Srinivasa Ramanujan.

Laubenbacher and Pengelly (2010) provides more biographical information, and examines her work on Fermat's Last Theorem from original manuscripts and letters, none of which she published. Legendre expounds some of this work in his paper of 1823, and credits Sophie Germain with a theorem that now bears her name. However, the manuscripts and letters reveal a much larger 'grand plan' to attack Fermat's Last Theorem. Even though this was ultimately flawed, it is the first attempt to tackle Fermat's Last Theorem as a whole, rather than just for single exponent values. Del Centina (2008) contains commentaries and mostly untranslated text of many of Sophie Germain's unpublished manuscripts, and provides more mathematical detail than Laubenbacher and Pengelly (2010). This reference shows how ambitious her plan was; it includes results which were lost, and only rediscovered 70 or more years later, and shows how some of her proofs were far more extensive in scope than the published proofs of Legendre. This situation is somewhat similar to that of the discovery in Riemann's unpublished manuscripts of the Riemann–Siegel formula.

Sophie Germain's work considers $x^p + y^p = z^p$ for odd primes p. Since $(-z)^p = -z^p$, it is equivalent to consider $x^p + y^p + z^p = 0$, the form we shall use from now on.

Part II will appear in M500 **273**

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 stated her theorem with the 2a condition, and to this day, primes p for which $2p + 1$ is also prime are known as Sophie Germain primes. Legendre used and acknowledged Sophie Germain's work, but stated it with the 2b condition. Implicit in 2a is the assumption that only primes of the form $2Np+1$ satisfy the condition. This was only proved in 1894. More startling is that if it could be shown that an infinite number of auxiliary primes $q = 2Np + 1$ existed for a particular N, then xyz would have to be infinite, hence proving Fermat's Last Theorem, not just case 1. This is because condition 2b implies that if $x^p + y^p + z^p = 0$, xyz must be divisible by q. Lastly, her version of the proof showed that for case 2, one of x, y, z is divisible by p^2, not just p. We will return to this later.

She proved case 1 of Fermat's Last Theorem for the primes between 3 and 193 (her manuscripts only claim up to 97), finding suitable q values by trial and error. With $N = 1$, 2, 4, 5, 7 or 8, the lowest such values are as in the following table.

p, N, q	p, N, q	p, N, q	p, N, q	p, N, q	p, N, q	p, N, q	p, N, q	p, N, q
3,1,7	17,4,137	37,2,149	59,7,827	79,2,317	103,5,1031	131,1,263	157,5,1571	181,5,1811
5,1,11	19,5,191	41,1,83	61,8,977	83,1,167	107,4,857	137,4,1097	163,2,653	191,1,383
7,2,29	23,1,47	43,2,173	67,2,269	89,1,179	109,5,1091	139,2,557	167,7,2339	193,2,773
11,1,23	29,1,59	47,7,659	71,4,569	97,2,389	113,1,227	149,4,1193	173,1,347	
13,2,53	31,5,311	53,1,107	73,2,293	101,4,809	127,2,509	151,5,1511	179,1,359	

We will see why multiples of 3 are excluded from the list of N values later.

As an example of a q that satisfies both conditions for a particular p, we will consider $p = 5, N = 1$, i.e. $q = 11$. The table of fifth powers for $q = 11$ is as follows.

$n \bmod 11$	0	1	2	3	4	5	6	7	8	9	10
$n^5 \bmod 11$	0	1	10	1	1	1	10	10	10	1	10

None of the $n^5 \bmod 11$ values is 5, so condition 1 is satisfied. Since $11 = 2\times5+1$, and the set of values of $n^5 \bmod 11$ contains no consecutive non-zero values, condition 2a is satisfied. Since the only values in the set are 0, 1 and 10, we can easily tabulate all x^5, y^5, z^5, $x^5+y^5+z^5 \bmod 11$ values, relabelling x, y, z if necessary so that $(x^5 \bmod 11) \le (y^5 \bmod 11) \le (z^5 \bmod 11)$:

$x^5 \bmod 11$	0	0	0	0	0	0	1	1	1	10
$y^5 \bmod 11$	0	0	0	1	1	10	1	1	10	10
$z^5 \bmod 11$	0	1	10	1	10	10	1	10	10	10
$x^5 + y^5 + z^5 \bmod 11$	0	1	10	2	0	9	3	1	10	8

The two cases where $x^5 + y^5 + z^5 \equiv 0 \bmod 11$ are $0, 0, 0$ and $0, 1, 10$. In the first case, each of x, y, z must be divisible by 10, so x, y and z are not relatively prime, so we can ignore this. In the second case, x is divisible by 10, so condition 2b is satisfied.

The equivalence of conditions 2a and 2b

Before we start on the proof of Sophie Germain's theorem, we need to look at what equivalence there is between the various elements of conditions 2a and 2b. In particular, we look at the negation of those conditions (slightly weakened), and show that these conditions are equivalent. In the following, q is a prime, but n is any odd integer greater than 1, not necessarily prime.

Condition A: There exist a, b and c with abc not divisible by q, such that $a^n + b^n + c^n \equiv 0 \bmod q$ (the negation of 2b).

Condition B: There exist integers d, e, neither of which is divisible by q, such that $d^n \equiv (e^n + 1) \bmod q$.

Condition C: If $q = 2Nn+1$, there exist solutions u, v of $x^{2N} \equiv 1 \bmod q$ such that $v \equiv (u + 1) \bmod q$ (a stronger version of the negation of 2a).

Proof that A⇒B: Since c is not divisible by q, there are integers d and e,

neither of which is divisible by q, such that $cd+a \equiv 0 \bmod q$, $ce \equiv b \bmod q$. So $-(cd)^n + (ec)^n + c^n \equiv 0 \bmod q$. Since c is not divisible by q, we can divide out c^n to give $d^n \equiv (e^n + 1) \bmod q$.

Proof that B⇒A: This follows immediately since $(-d)^n + e^n + 1^n \equiv 0 \bmod q$.

Proof that B⇒C: Let $u \equiv e^n \bmod q$, $v \equiv d^n \bmod q$. Then $u^{2N} \equiv e^{q-1} \equiv 1 \bmod q$ by Fermat's Little Theorem. Similarly, $v^{2N} \equiv d^{q-1} \equiv 1 \bmod q$.

Proof that C⇒B: Let f be a *primitive root* of q, i.e. $f^h \equiv 1 \bmod q$ for $h = q-1$, but for no smaller positive value of h. Let $u \equiv f^m \bmod q$, so that $f^{2Nm} \equiv u^{2N} \equiv 1 \bmod q$ by definition. Since f is a primitive root of the prime q, $f^h \equiv 1 \bmod q$ for $h = q-1 = 2Nn$, but for no smaller positive value of h; so m must be a multiple of $n = mg$, say. So $u \equiv (f^g)^n \equiv e^n \bmod q$, say. Similarly, $v \equiv d^n \bmod q$, say. But $v \equiv (u+1) \bmod q$, so $d^n \equiv (e^n+1) \bmod q$.

Since we have proved that A ⇔ B ⇔ C, we have also proved that $\bar{\text{A}} \Leftrightarrow \bar{\text{B}} \Leftrightarrow \bar{\text{C}}$, showing that conditions 2a and 2b are equivalent.

Clearly, the 2a condition has a direct connection to the prime p for which we are attempting to prove case 1. However, the 2b condition provides a relatively simple proof of Sophie Germain's theorem, which we finally get round to doing in the next section.

Legendre's proof of Sophie Germain's theorem, using condition 2b

We consider $x^p + y^p + z^p = 0$, allowing x, y and z to be interchanged freely when required. We require that x, y and z have been reduced so that $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$. We will show that if conditions 1 and 2b apply, then if none of x, y, z are divisible by p, $x^p + y^p + z^p = 0$ has no non-zero integer solutions.

We have $(-x)^p = y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + y^{p-3}z^2 - \cdots + z^{p-1}) = ab$, say, where $a = (y + z)$, $b = (y^{p-1} - y^{p-2}z + y^{p-3}z^2 - \cdots + z^{p-1})$. If q was a prime factor of both a and b (and so also a factor of x), we would get $y + z \equiv 0 \bmod q$ from a. Applying this to b, we would get $py^{p-1} \equiv 0 \bmod q$, giving $p \equiv 0 \bmod q$, or $y \equiv 0 \bmod q$. The first case implies $p = q$, since both are primes, but this would imply p was a factor of x. The second case implies $z \equiv 0 \bmod q$, which would imply $\gcd(y, z) > 1$, a contradiction. We have therefore shown $\gcd(a, b) = 1$. Since $ab = (-x)^p$, both a and b must be pth powers (a, b must each be the product of pth powers of primes, none of which are common to both a and b). Applying similar arguments for $(-y)^p = x^p + z^p, (-z)^p = x^p + y^p$, there must be integers a, b, c, d, e, f such that

A: $y+z=a^p$, $y^{p-1}-y^{p-2}z+y^{p-3}z^2-\cdots+z^{p-1}=b^p$, $x=-ab$,
B: $z+x=c^p$, $z^{p-1}-z^{p-2}x+z^{p-3}x^2-\cdots+x^{p-1}=d^p$, $y=-cd$,
C: $x+y=e^p$, $x^{p-1}-x^{p-2}y+x^{p-3}y^2-\cdots+y^{p-1}=f^p$, $z=-ef$.

Condition 2b requires that one of x, y, z is divisible by q. Relabel if necessary so that $x \equiv 0 \bmod q$. Then $2x = (x+z)+(y+x)-(y+z) = c^p+e^p+(-a)^p \equiv 0 \bmod q$. Applying condition 2b again, one of a, c, e is divisible by q. If c or e were divisible by q, we would have $y=-cd \equiv 0 \bmod q$, or $z=-ef \equiv 0 \bmod q$, but we already have $x \equiv 0 \bmod q$, so $\gcd(x,y)>1$ or $\gcd(x,z)>1$, contradicting our requirement.

If, instead, a were divisible by q, we would get $y \equiv -z \bmod q$, $b^p \equiv py^{p-1}$ from A. From C, $y^{p-1} = f^p \bmod q$, so $pb^p \equiv f^p \bmod q$. Since $b \not\equiv 0 \bmod q$, there is an integer g such that $bg \equiv 1 \bmod q$, so that $p(bg)^p \equiv p \equiv (fg)^p \bmod q$, contradicting condition 1, hence no solution exists.

The p^2 result from Sophie Germain's own proof

Sophie Germain did not identify the theorem that bears her name as an entity in its own right. Rather, her proof emerges during paragraphs that aim to demonstrate the huge size of any possible solutions to Fermat's Last Theorem. Unfortunately, there is a flaw in her proof, which unpublished manuscripts suggest she recognized and was trying to correct (details can be found in Laubenbacher and Pengelley (2010) sections 4.1.1 to 4.1.3). However, she did show that if conditions 1 and 2a are satisfied, then if any solutions of $x^p+y^p+z^p=0$ exist, one of x, y, z must be divisible by p^2, not just p. The following is an adaptation of her proof of this, using the scheme set out in Legendre's proof in the previous section.

Without loss of generality, we assume that x is divisible by p. Since $\gcd(x,y)=\gcd(x,z)=1$, neither y nor z can be divisible by p. By Fermat's Little Theorem, $y^{p-1} \equiv 1 \bmod p$, so $y(y^{p-1}-1) = y^p - y$ is divisible by p. Similarly, $z^p - z$ is divisible by p, so adding, we get $(y^p+z^p) \equiv (y+z) \bmod p$. But $y^p+z^p \equiv -x^p \equiv 0 \bmod p$, so $y+z$ is divisible by p. We have

$$(-x)^p \;=\; y^p+z^p \;=\; (y+z)(y^{p-1}-y^{p-2}z+y^{p-3}z^2-\cdots+z^{p-1}) \;=\; ab,$$

say, where $a=(y+z)$, $b=(y^{p-1}-y^{p-2}z+y^{p-3}z^2-\cdots+z^{p-1})$. So

$$b=\frac{y^p+(a-y)^p}{a}=a^{p-1}-\binom{p}{1}a^{p-2}y+\cdots-\binom{p}{p-2}ay^{p-2}+\binom{p}{p-1}y^{p-1}.$$

Since p is prime, $\binom{p}{n}$ is divisible by p for $1 \le n \le p-1$, and since $a=y+z$ is divisible by p, all the terms in the expression for b above are divisible by

p^2 apart from $\binom{p}{p-1}y^{p-1} = py^{p-1}$, so b is divisible by p, but not divisible by any higher power of p.

From the previous section, we had

A: $y + z = a^p$, $y^{p-1} - y^{p-2}z + y^{p-3}z^2 - \cdots + z^{p-1} = b^p$, $x = -ab$,

B: $z + x = c^p$, $z^{p-1} - z^{p-2}x + z^{p-3}x^2 - \cdots + x^{p-1} = d^p$, $y = -cd$,

C: $x + y = e^p$, $x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots + y^{p-1} = f^p$, $z = -ef$.

Adding B and C, we get $2x + (y + z) = c^p + e^p$. Since x and $(y + z)$ are both divisible by p, $c^p + e^p$ is divisible by p. Since neither y nor z is divisible by p, neither $c^p = z + x$ nor $e^p = x + y$ is divisible by p, so by the same argument used for y, z above, we have $c + e$ is divisible by p. So $c = Kp - e$ for some K. Then

$$c^p \;=\; (-e + Kp)^p \;=\; -e^p + \binom{p}{1}pK(-e)^{p-1} + \binom{p}{2}p^2K^2(-e)^{p-2} + \ldots,$$

with all additional terms divisible by p^2, so $c^p + e^p$ is divisible by p^2. Since x is divisible by p, $ab = (-x)^p = y^p + z^p$ is divisible by p^p. Since b is divisible by p but not by any higher power of p, a is divisible by p^{p-1}, hence a^p is divisible by $p^{p(p-1)}$. Since $p(p-1) > 2$ for all $p > 2$, a^p is divisible by p^2. Adding B and C above, then subtracting A, we get $2x = (c^p + e^p) - a^p$, so x is divisible by p^2 for $p > 2$.

Legendre's approach to generalization

Since we have shown that conditions 2a and 2b are equivalent, and Legendre's proof is valid for condition 2b, it follows that if q is an auxiliary prime of the form $2Np + 1$, and conditions 1 and 2a apply, then the theorem is proved for p. A suitable q could be found by trial and error for a particular p. It would be far better if we can show for particular values of N whether the conditions are always satisfied, sometimes satisfied, or never satisfied. We now show that the conditions are always satisfied for $N = 1, 2, 4, 5, 7$ and 8 (these are the lowest N values that cover all the primes up to 193—see the table on page 8 for details).

Before proceeding further, we need some conditions which are equivalent to condition 1 for q of the form $2Np + 1$:

A $n^p \not\equiv p \bmod q$ for all integers n (condition 1 itself),

B $(2N)^{2N} \not\equiv 1 \bmod q$,

C $p^{2N} \not\equiv 1 \bmod q$.

Proof that $\bar{\mathrm{B}} \Rightarrow \bar{\mathrm{A}}$: Let f be a primitive root of q, and let $p \equiv f^R \bmod q$. If $(2N)^{2N} \equiv 1 \bmod q$, then $f^{NR} \equiv p^{2N} \equiv (2Np)^{2N} \equiv (q-1)^{2N} \equiv (-1)^{2N} \equiv$

1 mod q. Since q is prime, $2NR$ must be a multiple of $(q-1) = 2Np$ by Fermat's Little Theorem, so R must be a multiple of p. Denoting $a \equiv f^{R/p} \bmod q$, we have $a^p \equiv f^R \equiv p \bmod q$.

Proof that $\bar{\mathrm{A}} \Rightarrow \bar{\mathrm{C}}$: If there is an a such that $a^p \equiv p \bmod q$, then $p^{2N} \equiv a^{2Np} \equiv a^{q-1} \equiv 1 \bmod q$.

Proof that $\bar{\mathrm{C}} \Rightarrow \bar{\mathrm{B}}$: If $p^{2N} \equiv 1 \bmod q$, then $(2N)^{2N} \equiv (2N)^{2N} p^{2N} \equiv (q-1)^{2N} \equiv 1 \bmod q$.

We have shown $\bar{\mathrm{B}} \Rightarrow \bar{\mathrm{A}} \Rightarrow \bar{\mathrm{C}} \Rightarrow \bar{\mathrm{B}}$, so $\mathrm{A} \Leftrightarrow \mathrm{B} \Leftrightarrow \mathrm{C}$. We need another definition before starting on the proofs: a is a *primitive nth root of* 1 *modulo* p if $a^n \equiv 1 \bmod p$, and the set $\{1, a, a^2, \ldots, a^{n-1} \bmod p\}$ are all distinct. Primitive nth roots only exist if n is a factor of $(p-1)$. We also need the following: If w is a primitive nth root of 1 modulo p, and c is such that $\gcd(c, p-1) = 1$, then $w^c \bmod p$ is also a primitive nth root (since its set is formed by picking every cth element of $\{1, a, a^2, \ldots, a^{n-1} \bmod p\}$, cycling round if necessary).

The following proofs are due to Legendre. His approach is to tackle one value of N at a time. We will then have a look at Sophie Germain's approach, which is more radical.

$N = 1 : q = 2p + 1$

If condition 1 is not satisfied, $a^p \equiv p \bmod q$ for some a. From B above, we have shown that this is equivalent to $(2N)^{2N} \equiv 1 \bmod q$, i.e. $4 \equiv 1 \bmod q$. Since q is prime, $q = 3$, giving $p = 1$, which is excluded, so condition 1 is always satisfied. Since q is a prime, we have $a^{q-1} \equiv 1 \bmod q$ for any $0 < a < q$. This means $a^{(q-1)/2} \equiv a^p \equiv \pm 1 \bmod q$. If condition 2b does not apply, there are a, b, c with abc not divisible by q, such that $a^p + b^p + c^p \equiv 0 \bmod q$, but we know $a^p + b^p + c^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \bmod q$, since $q > 3$, so condition 2b is always satisfied. We have therefore proved case 1 of Fermat's Last Theorem for $p = 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, \ldots$.

$N = 2 : q = 4p + 1$

If condition 1 is not satisfied, $a^p \equiv p \bmod q$ for some a. From B above, we have shown that this is equivalent to $(2N)^{2N} \equiv 1 \bmod q$, i.e. $4^4 = 256 \equiv 1 \bmod q$, i.e. q is a factor of $255 = 3 \times (4 \times 1 + 1) \times (4 \times 4 + 1)$, for which p would have to be 1 or 4, an impossibility, so condition 1 is always satisfied.

Let w be a primitive fourth root of 1 modulo q, i.e. $w^4 \equiv 1 \bmod q$, $w^2 \equiv -1 \bmod q$, $w^3 = -w \bmod q$. If condition 2a does not apply, there must be u, v such that $u^{2N} \equiv v^{2N} \equiv 1 \bmod q, v \equiv (u+1) \bmod q$ (see condition C on page 8). We therefore have to check which combinations of roots can give rise to such u, v:

$1, w : w \equiv 2 \bmod q$.

$1, w^2$: Since $w^2 \equiv -1 \bmod q$, this cannot apply.

$1, w^3 : w^3 = -w \bmod q$, so this is equivalent to $w \equiv -2 \bmod q$.

$w, w^2 : w^2 = -1 \bmod q$, so this is equivalent to $w \equiv -2 \bmod q$.

$w, w^3 : w^3 = -w \bmod q$, so this is equivalent to $w \equiv -w \pm 1 \bmod q$, i.e. $2w \equiv \pm 1 \bmod q$.

w^2, w^3 : This is equivalent to $-1, -w$, giving $w \equiv 2 \bmod q$.

So we have either $w \equiv \pm 2 \bmod q$, or $2w \equiv \pm 1 \bmod q$. Squaring the first alternative gives $w^2 \equiv 4 \bmod q$, but $w^2 \equiv -1 \bmod q$. Squaring the second alternative gives $4w^2 \equiv 1 \bmod q$, but $4w^2 \equiv -4 \bmod q$. In either case, this implies $q = 5$, giving $p = 1$. We have therefore proved case 1 of Fermat's Last Theorem for $p = 7$, 13, 37, 43, 67, 73, 79, 97, 127, 139, 163, 193, ... The cases $N = 4$, 5, 7, 8 are covered in Ribenboim (1991) section IV.1 1E. In these cases, condition 1 is satisfied for all p. This is not always true (probably not too surprisingly), as the next example shows.

$N = 3 : q = 6p + 1$ – a cautionary tale

If condition 1 is not satisfied, $a^p \equiv p \bmod q$ for some a. From B above, we have shown that this is equivalent to $(2N)^{2N} \equiv 1 \bmod q$, i.e. $6^6 = 46656 \equiv 1 \bmod q$, i.e. q is a factor of $46655 = 5 \times 7 \times 31 \times 43$. Of these factors, $31 = 6 \times 5 + 1$, $43 = 6 \times 7 + 1$, so condition 1 is not satisfied for $p = 5$, $p = 7$.

If condition 2a is not satisfied, we check as before which combinations of roots give rise to u, v such that $u^{2N} \equiv v^{2N} \equiv 1 \bmod q$, $v \equiv (u+1) \bmod q$. One such combination requires $w^2 \equiv w - 1 \bmod q$, where w is a primitive sixth root of 1 modulo q. Multiplying by w gives $w^3 \equiv w^2 - w \equiv -1 \bmod q$, so providing no constraints on q; so we cannot use $N = 3$ (or indeed any multiple of 3) to prove case 1 of Fermat's Last Theorem for any p.

References

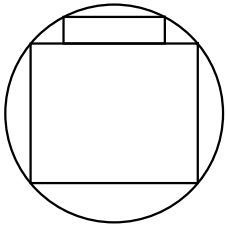
Del Centina, A. (2008), 'Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's Last Theorem', *Archive for the History of Exact Sciences* Vol. 62 No. 4, pp 349–392.

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, pp 641–692.

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

Solution 269.2 – Two rectangles



Two rectangles are packed inside a circle of radius 1. What is the largest area they can occupy?

Tony Forbes

Strictly speaking, this might not be a solution to the stated problem because I make the assumption that there is a big rectangle, whose vertices are on the circle, together with a small rectangle sitting on top—as in the diagram. My reason is simply that I cannot see how any other way of arranging the rectangles would work better.

Mike Shaw sent a solution based on the big rectangle being a $\sqrt{2}\times\sqrt{2}$ square and obtained

$$2+\frac{1}{8}\left(\sqrt{46-2\sqrt{17}}-2\sqrt{14-2\sqrt{17}}\right) \;\approx\; 2.168375 \tag{1}$$

for the largest enclosed area. However, I find that by squashing the square a little we can increase the total area to about 2.195184. I would be very interested if anyone can improve on this last value with some imaginative arrangement of the rectangles.

Denote the *height* of the big rectangle by $2b$. Then its width is $2\sqrt{1-b^2}$ and its area is $4b\sqrt{1-b^2}$. Denote the *width* of the small rectangle by $2x$ so that it has height $\sqrt{1-x^2}-b$ and area $2x(\sqrt{1-x^2}-b)$.

Let us fix b for now and concentrate on getting a function $x_{\max}(b)$ of $b\in[0,1]$ for the half-width of the small rectangle of largest area. Consider the equation

$$\frac{\partial}{\partial x}\big(\text{area of small rectangle}\big) \;=\; \frac{\partial}{\partial x}2x\left(\sqrt{1-x^2}-b\right) \;=\; 0,$$

or $1-2x^2=b\sqrt{1-x^2}$, which on squaring becomes

$$4x^4+(b^2-4)x^2+1-b^2 \;=\; 0. \tag{2}$$

Solving (2) we have $x=\pm\sqrt{4-b^2\pm b\sqrt{8+b^2}}/(2\sqrt{2})$, and of these four solutions the only one we really want is

$$x_{\max}(b) \;=\; \frac{\sqrt{4-b^2-b\sqrt{8+b^2}}}{2\sqrt{2}}.$$

When we substitute $x_{\max}(b)$ for x in $2x\left(\sqrt{1-x^2}-b\right)$ we obtain

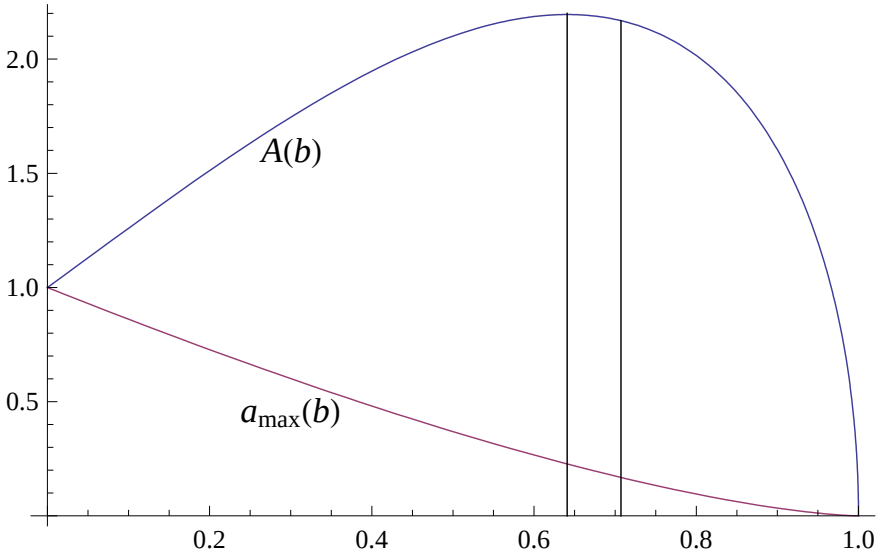
$$a_{\max}(b) \;=\; \frac{1}{4}\sqrt{4-b^2-b\sqrt{8+b^2}}\left(\sqrt{4+b^2+b\sqrt{8+b^2}}-\sqrt{8}\,b\right)$$

for the maximum area of the small rectangle given that the big rectangle has height $2b$. You can also check that $2 + a_{\max}(\sqrt{2}/2)$ reproduces the expression in (1).

We want to find $b_{\max}$, the value of b that maximizes the total area,

$$A(b) \;=\; 4b\sqrt{1-b^2} + a_{\max}(b).$$

By plotting $A(b)$ we see several interesting things. The graph ends at $A(1) = 0$, where our 'big' rectangle has become very thin, and starts at $A(0) = 1$, where it degenerates into a horizontal line and the best we can do is place a 'small' $\sqrt{2} \times \sqrt{2}/2$ rectangle on top of it. The first vertical line indicates where $A(b)$ is at its maximum and the second line, slightly away from the true maximum, marks the spot where $b = \sqrt{2}/2$ and the big rectangle is a square.



Now for the messy part. We solve $dA(b)/db = 0$ for b. This is obviously a task for MATHEMATICA and so the details are omitted. The result is that the optimum area occurs at

$$b_{\max} \;=\; \frac{1}{12}\sqrt{\frac{539+\rho^2 q+\rho p}{7}} \;=\; 0.64089199521794561146\ldots,$$

where

$$\begin{aligned}
\rho &= -\frac{1}{2}+\frac{\sqrt{3}\,i}{2}, \quad \text{a cube root of 1,}\\
p &= \left(7\left(-25627+144\sqrt{43827}\,i\right)\right)^{1/3} \;\approx\; 47.317635+44.833486\,i \;\text{ and}\\
q &= \left(7\left(-25627-144\sqrt{43827}\,i\right)\right)^{1/3} \;\approx\; 47.317635-44.833486\,i
\end{aligned}$$

with the cube roots chosen such that p and q have the stated approximate values. Observe that p and q are conjugates; therefore $b_{\max}$ is real, as it should be. Also the product is an integer, $pq = 7 \cdot 607$.

To get the maximum area, all we do is compute $A(b_{\max})$. Let

$$\begin{aligned}
r &= \rho^2 q+\rho p \;\approx\; -124.971510,\\
u &= \sqrt{539+r} \;\approx\; 20.347690,\\
v &= \sqrt{469-r} \;\approx\; 24.371531,\\
w &= r+\sqrt{8603+r}\,u \;\approx\; 1748.566676,
\end{aligned}$$

and notice that all four numbers are real. Then

$$\begin{aligned}
A(b_{\max}) &= \frac{uv}{252}+\frac{\sqrt{3493-w}}{16\cdot 252}\left(-2\sqrt{2}\,u+\sqrt{4571+w}\right)\\
&= 2.19518381298757987668\ldots,
\end{aligned}$$

which breaks down as follows.

	width	height	area
big rectangle	1.5352621280…	1.2817839904…	1.9678744168…
small rectangle	0.9302119692…	0.2443630093…	0.2273093961…

I put this rather complicated maximization problem in M500 because I was very surprised to find that the big rectangle is not square. However, I can't make up my mind whether or not I should have been.

Solution 270.5 – Binomial coefficient sum

Integers n and k satisfy $k > n \geq 0$. Show that

$$\sum_{j=0}^{k}(-1)^j\binom{k}{j}j^n \;=\; 0.$$

One way of getting this result is via the recursion formula for Stirling numbers of the second kind. However, we are really interested in a simple, direct proof.

Dave Wild

Using the Binomial Theorem we have

$$(1-e^x)^k \;=\; \sum_{j=0}^{k}(-1)^j\binom{k}{j}e^{jx}.$$

Using the power series for the exponential function gives

$$\left(-\sum_{i=1}^{\infty}\frac{x^i}{i!}\right)^k \;=\; \sum_{j=0}^{k}(-1)^j\binom{k}{j}\sum_{i=0}^{\infty}\frac{(jx)^i}{i!}.$$

Defining $0^0 = 1$ and equating powers of x^n, where $0 \leq n < k$, gives

$$0 \;=\; \sum_{j=0}^{k}(-1)^j\binom{k}{j}\frac{j^n}{n!}.$$

Multiplying both sides by $n!$ gives the required result.

Letter

Dear Eddie,

I thought your piece on Man Ray [M500 **270**] was interesting, and I hadn't known about his photographs of mathematical models. Found some on the web, and there is more to them than I had supposed. On the other hand, Man Ray's response to them was the kind of thing you would expect from a fluff-headed artist, surrealist or otherwise: just photograph or draw them, then give them silly names. *New Scientist* sometimes has reviews of art exhibitions inspired by science, and tries to present them as meaningful, culturally significant and so on, but they always seem to be the same thing, artists playing rather feebly with things they don't understand.

Ralph Hancock

Napier's logarithms are hyperbolic after all

Peter L. Griffiths

Napier recognized that the formula for the hyperbola,

$$\frac{1}{1+x} \;=\; 1 - x + x^2 - x^3 + \ldots,$$

could be converted into measuring the area under the hyperbola by integration similar to the conversion of the circumference of a circle, $2\pi r$, into the area of the circle, πr^2:

$$\int \frac{dx}{1+x} \;=\; x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots.$$

Multiplying both sides by $1/2$ gives

$$\frac{1}{2}\int \frac{dx}{1+x} \;=\; \frac{x}{2} - \frac{x^2}{4} + \frac{x^3}{6} - \frac{x^4}{8} + \ldots.$$

Napier very cleverly recognised that $\int dx/(1+x)$ could be represented as $\log(1+x)$, so that $1/2\int dx/(1+x)$ could be represented as $1/2\log(1+x)$ or $\log(1+x)^{1/2}$. In this way, with $x = 1$,

$$\log 2 \;=\; 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots \;=\; 0.693147,$$

and $\log 2^{1/2} = 1/2 - 1/4 + 1/6 - 1/8 + \cdots = 0.346574$. Napier mentions amounts close to 0.693147 and 0.346574 in paragraphs 46–53 of the *Constructio*. He also refers to $0.9999999^{346574} = 0.965936288$, which is approximately sine 75 degrees, in the formula in paragraph 44.

Problem 272.1 – Finite integral

Show that

$$\int_0^{2\pi} (\cos x)\left(\sin\frac{x}{2}\right)\left(\tan\frac{x}{3}\right) dx \;=\; \frac{-18\sqrt{3}}{5}.$$

Problem 272.2 – Infinite integral

Show that

$$\int_0^{\infty} e^{-x}(\log x)\, dx \;=\; -\gamma \;=\; -0.5772156649\ldots.$$

Problem 272.3 – Stamps

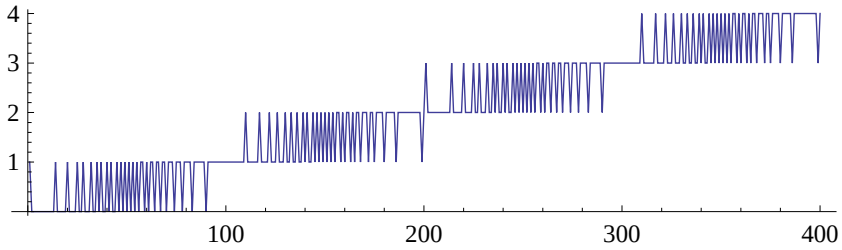
Tony Forbes

Every week a publisher posts that week's issue of a magazine to each of its subscribers. In week 1 there is just one subscriber. But the Post Office sells stamps only in sheets of 100. So 100 stamps are bought, one is used and 99 are left over for future weeks. In week 2 another subscriber joins; so there are two magazines to post and 97 stamps remain. In week 3 ... I expect you can guess what happens.

In week n there are n magazines to post and $100\,s(n)$ stamps need to be purchased. Show that $s(n + 200) = s(n) + 2$ for $n \geq 1$ and that $s(200 - n) = 2 - s(n)$ for $1 \leq n < 200$.

In case it helps, here is what $s(n)$ looks like for $n \leq 32$ and for $n \leq 400$.

$$1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, \ldots$$



Problem 272.4 – Pseudoprimes

Tony Forbes

A *pseudoprime* is a composite number n that satisfies $2^n \equiv 2 \pmod{n}$. Odd pseudoprimes are not common, but also they are not particularly rare. Even pseudoprimes are somewhat rarer—only 20 less than 10^9 ...

161038	215326	2568226	3020626	7866046
9115426	49699666	143742226	161292286	196116194
209665666	213388066	293974066	336408382	377994926
410857426	665387746	667363522	672655726	760569694

... and you will note that they are all congruent to 2 modulo 4. Why? More generally, find a pseudoprime that is divisible by p^2 for some prime p, or prove than none exist.

M500 Winter Weekend 2017

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

Florence Boot Hall, **Nottingham University**

Friday 6th – Sunday 8th January 2017.

Cost: £210 to M500 members, £215 to non-members. This includes accommodation and all meals from dinner on Friday to lunch on Sunday. You can obtain a booking form either from the M500 web site,

http://www.m500.org.uk,

or by emailing the Winter Weekend Organizer at winter@m500.org.uk.

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.

M500 Mathematics Revision Weekend 2017

The M500 Revision Weekend 2017 will be held at

Kents Hill Park Training and Conference Centre,

Milton Keynes, MK7 6BZ

from Friday 12th to Sunday 14th May 2017.

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, and are included with this magazine mailing for those who did not.

Contact the Revision Weekend Organizer, **Judith Furner**, at email address weekend@m500.org.uk if you have any queries about this event.

Problem 272.5 – Sums of digits of powers

Given an integer n, can you always find integers b, $2 \leq b < n$ and $k \geq 2$ such that n is equal to the sum of the base-b digits of n^k?

If we fix the base to $b = 10$, this doesn't always work. For example, 1827 is the sum of the digits of 1827^{121}, 1828 is the sum of the digits of 1828^{123} and 1829 is the sum of the digits of 1829^{121}, but there is no corresponding relation for 1830.

Advice for authors

Over the next few months I (TF) am likely to be busier than usual. I shall therefore attempt to reduce my workload by offering some helpful guidelines for contributors to M500.

Please read recent issues of the magazine and please conform to its style. Please also note that M500 is printed using only black ink and that the text block is only 115 mm wide.

Plain English is preferred. Avoid unreasonable use of symbols. So write 'for all positive integers n' rather than '$\forall n \in \mathbb{Z}^+$', 'therefore' instead of '$\therefore$', etc. Do not start a sentence with a symbol, or a word like 'calorie'. Do not use theorems, pictures, tables, etc. as nouns. Try to avoid more than one level of subscripting or superscripting. Avoid redundant brackets, non-standard fonts for variables and bizarre deviations from standard mathematical presentation. Avoid spoon-feeding.

LaTeX This is the preferred option. I suggest you download the TeX file for these notes from the M500 web site (or ask me for it) and adapt it for your own use. Here are a few rules. Please comply with them.

Ensure there is extra space on both sides of the main symbol in displayed mathematics. For example, write '$\sim=\sim 1$' rather than '$=1$' in

$$\cos^2\theta + \sin^2\theta \;=\; 1.$$

Ensure that mathematical items are properly separated. Remember that in math mode a comma is not followed by any space; so, for example, write '$a=1$, $b=2$, $c=3$' rather than '$a=1, b=2, c=3$'. Use '\dots' rather than '...'. Use '\cdot' or '\times' for explicit multiplication. A decimal point is an ordinary full stop. Reset the appropriate counters if you are automatically numbering equations, etc. Ensure that LaTeX commands you define won't clash with existing commands.

Other word processors The existence of non-LaTeX word processors is an unfortunate complication because I usually have to convert mathematical constructs by hand. This might explain to some authors why their contributions get held up. So I have to ask: Please try to avoid symbols that are not on the keyboard. Fortunately, plain English requires hardly any additional work and is very much preferred.

Remember to send me the PDF file of your article as well as the word processor document. A warning: I cannot deal with a long article where much of the text is inaccessible to copy-and-paste; I would have to ask you to get it converted to LaTeX.

04.00

Problem 272.6 – Irreducible polynomials

Tony Forbes

Suppose a and $b > a$ are positive integers with $\gcd(a, b) = 1$. Observe that $x^{a+b} - 2x^b + 1$ is divisible by $x - 1$. Observe also that

$$x^7 - 2x^5 + 1 \;=\; (x-1)(x^3 - x - 1)(x^3 + x^2 + 1).$$

Either show that this is the only case where $(x^{a+b}-2x^b+1)/(x-1)$ factorizes into polynomials with integer coefficients, or find another example.

Front cover Five triangles (page 5).