MATHEMATICAL MAYHEM

Mathematical Mayhem began in 1988 as **a Mathematical Journal for and by High School and University Students**. It continues, with the same emphasis, as an integral part of ***Crux Mathematicorum with Mathematical Mayhem***.

All material intended for inclusion in this section should be sent to Mathematical Mayhem, Department of Mathematics, University of Toronto, 100 St. George St., Toronto, Ontario, Canada. M65 3G3. The electronic address is

mayhem@math.toronto.edu

The Assistant Mayhem Editor is Cyrus Hsia (University of Western Ontario). The rest of the staff consists of Adrian Chan (Harvard University), Jimmy Chui (University of Toronto), Donny Cheung (University of Waterloo), and David Savitt (Harvard University)

Mayhem Problems

The Mayhem Problems editors are:

Adrian Chan	*Mayhem High School Problems Editor,*
Donny Cheung	*Mayhem Advanced Problems Editor,*
David Savitt	*Mayhem Challenge Board Problems Editor.*

Note that all correspondence should be sent to the appropriate editor — see the relevant section. In this issue, you will find only problems — the next issue will feature only solutions.

We warmly welcome proposals for problems and solutions. With the schedule of eight issues per year, we request that solutions from this issue be submitted in time for issue 8 of 2001.

High School Problems

Editor: Adrian Chan, 1195 Harvard Yard Mail Center, Cambridge, MA, USA 02138-7501 <ahchan@fas.harvard.edu>

H277.

(a) Find all right triangles with integer sides with perimeter 60.

(b) Find all right triangles with integer sides with area 600.

H278. Consider the time as seen on a digital clock in 24 hour mode. (24 hour mode is representing the time relative to 12 midnight. For example, 6:25 am is 06:25, but 6:25 pm is 18:25. Also, 12:45 am counts as 00:45.) Let n be the number we get when we remove the colon from the time T as seen on a digital clock in 24 hour mode. Find all times T such that:

(i) n is a palindrome, [Ed. reads the same backwards as forwards.]

(ii) m, the number of minutes that T is after midnight, is a palindrome, and

(iii) $n = m$.

H279. *Proposed by Ho-joo Lee, student, Kwangwoon University, Kangwon-Do, South Korea.*

Let a and b be integers such that $a \equiv b \pmod 3$. Prove that

$$\tfrac{2}{3}\ \left(a^2 + ab + b^2\right)$$

can be expressed as a sum of three non-negative squares.

H280. *Proposed by Fotifo Casablanca, Bogotá, Colombia.*

In the spirit of the Olympics: There are 9 regions inside the rings of the Olympics. Put a different positive whole number in each so that the five products of the numbers in each ring form a set of five consecutive integers.

Advanced Problems

Editor: Donny Cheung, c/o Conrad Grebel College, University of Waterloo, Waterloo, Ontario, Canada. N2L 3G6 <dccheung@uwaterloo.ca>

A253. *Proposed by Mohammed Aassila, Strasbourg, France.*

Does there exist a polynomial $f(x, y, z)$ with real coefficients, such that $f(x, y, z) > 0$ if and only if there exists a non-degenerate triangle with side lengths $|x|$, $|y|$, and $|z|$?

A254. In the acute triangle ABC, the bisectors of $\angle A$, $\angle B$, and $\angle C$ intersect the circumcircle again at A_1, B_1 and C_1, respectively. Let M be the point of intersection of AB and B_1C_1, and let N be the point of intersection of BC and A_1B_1. Prove that MN passes through the incentre of triangle ABC.

(1997 Baltic Way)

A255. *Proposed by Ho-joo Lee, student, Kwangwoon University, Kangwon-Do, South Korea.*

Define $A = (\sum_{i=1}^{n} a_i)/n$, $G = \sqrt[n]{\prod_{i=1}^{n} a_i}$, and $H = n/(\sum_{i=1}^{n} 1/a_i)$ for positive real numbers a_1, a_2, $\ldots$, a_n. It is known that $A \geq G \geq H$, from which it follows that $0 \geq \log(G/A)$ and $0 \geq 1 - A/H$. Prove that $0 \geq \log(G/A) \geq 1 - A/H$, and determine when equality holds.

A256. ~~*Proposed by Mohammed Aassila, Strasbourg, France*~~.

Prove that for any positive integer n, there exist $n+1$ points M_1, M_2, $\ldots$, M_{n+1} in $\mathbb{R}^n$ such that for any integers i and j for which $1 \leq i < j \leq n+1$, the Euclidean distance between M_i and M_j is 1.

Challenge Board Problems

Editor: David Savitt, Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA, USA 02138 <dsavitt@math.harvard.edu>

C97. Given a positive integer n, let $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{n-1}$ denote the integers modulo n (so that $\overline{a}$ is the reduction of a modulo n). Find all positive integers n with the property that the set

$$\{\overline{a} \mid 0 < a < n/2 \text{ with } a \text{ and } n \text{ relatively prime}\}$$

is a group under multiplication.

C98. Find all pairs of integers (x, y) which satisfy the equation

$$x^2 - 34y^2 = -1 .$$

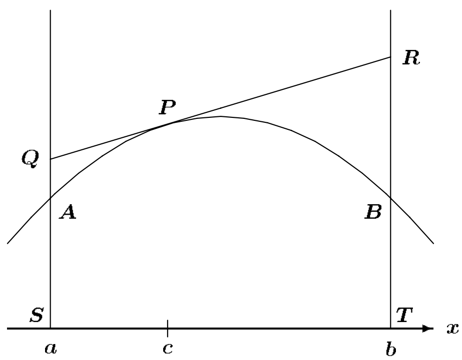
Problem of the Month

Jimmy Chui, student, University of Toronto

Problem. The graph of the function $y = f(x)$ is concave downward over the interval $a \le x \le b$. A and B are the points $(a, f(a))$, $(b, f(b))$, respectively. The tangent to $y = f(x)$ at any point $P(x, f(x))$, $a \le x \le b$, meets the line $x = a$ at Q and the line $x = b$ at R. If the area bounded by the curve, the tangent at P, the line $x = a$, and the line $x = b$, is minimized, prove that the x–coordinate of the point P is independent of the function $f(x)$.

(1997 Descartes, Problem 12)

Solution.



Let P be at $(c, f(c))$. Let S and T be the points $(a, 0)$ and $(b, 0)$, respectively. Without loss of generality, we can assume that the points A, B, P, Q, and R, lie above the x-axis. (If they do not, we can merely translate the points upward until they do lie above the x-axis, and this translation will not affect the area in question.)

Now, the area under the curve between $x = a$ and $x = b$ is fixed. Hence, we want to find the c such that the area of trapezoid $QRTS$ is a minimum.

The area of the trapezoid is $\frac{1}{2}(b - a)(Q_y + R_y)$, where Q_y and R_y are the y–coordinates of Q and R, respectively. But since $\frac{1}{2}(b - a)$ is constant, that only means we must find the c that yields the minimum value of $Q_y + R_y$. This is equivalent to finding the c that yields the minimum value of $\frac{1}{2}(Q_y + R_y)$; that is, the average value of the y–coordinates of Q and R.

Consider the tangent line $y = g(x)$. This tangent line varies with c. Because $f(x)$ is concave down, the line $g(x)$ lies entirely above $f(x)$ except at the contact point. In other words, $g(x) \ge f(x)$ with equality if and only if $x = c$.

Now $\frac{1}{2}(Q_y + R_y) = \frac{1}{2}(g(a) + g(b)) = g(\frac{a+b}{2})$, with the last equality holding since $g(x)$ is a linear function. But $g(\frac{a+b}{2}) \geq f(\frac{a+b}{2})$, with equality if and only if $c = \frac{a+b}{2}$. In turn, this means that the minimum value of $\frac{1}{2}(Q_y + R_y)$ is $f(\frac{a+b}{2})$, and this occurs only when $c = \frac{a+b}{2}$.

Hence, the area in question is minimized when $c = \frac{a+b}{2}$, which is independent of $f(x)$, QED.

Remark. This problem can also be solved using calculus.

J.I.R. McKnight Problems Contest 1986 — Solution

4. (b) Prove that in any acute triangle ABC,

$$\cot A + \cot B + \cot C = \frac{a^2 + b^2 + c^2}{4K},$$

where K is the area of triangle ABC.

Solution by Vedula N. Murty, Dover, PA, USA.

We use the following formulae:

$$\cos A = \frac{b^2 + c^2 - a^2}{2bc},$$

$\sin A = a/(2R)$, where R is the circumradius of the triangle ABC, and $K = abc/(4R)$.

From these, we have

$$\cot A = \frac{R(b^2 + c^2 - a^2)}{abc},$$

Using this equation and similar equations for $\cot B$ and $\cot C$, we have

$$\cot A + \cot B + \cot C = \frac{a^2 + b^2 + c^2}{4K}.$$

This appears to be a little simpler than the one given in [1999 : 296–297]. Now, why do we need the triangle to be acute?

Another Do-It-Yourself Proof of the $n = 3$ case of Fermat's Last Theorem

Andy Liu

Part Zero.

Everyone knows Fermat's Last Theorem, which states that the Diophantine equation $x^n + y^n = z^n$ has no solution in non-zero integers for all $n \geq 3$. This article offers a proof of the case $n = 3$ different from the one presented in [2]. The idea of the present proof is taken from [1], with two changes. First, the concept of quadratic residues, though very useful in general, would take us too far afield. It was discovered that the reference to quadratic residues in the argument in [1] is actually redundant, and is accordingly excised. Second, the main lemma in the argument in [1] is rather unmotivated. It is now presented in a manner which makes its discovery plausible.

Part One.

We wish to prove that the Diophantine equation $x^3 + y^3 = z^3$ has no solutions in non-zero integers. Our approach is indirect. Suppose that such a solution exists.

Problem 1.

Prove that no two of x, y and z are equal.

By the Well Ordering Principle, there exists a solution such that $|xyz|$ is minimal.

Problem 2.

Prove that x, y and z are pairwise relatively prime to one another, and that exactly one of them is even.

We will attempt to construct another solution for which $|xyz|$ is smaller. This will yield the desired contradiction. We may assume that z is even. Then $x + y$ and $x - y$ are both even. Hence, there exist integers u and w such that $x + y = 2u$ and $x - y = 2w$. It follows that $x = u + w$ and $y = u - w$. We then have $z^3 = (u + w)^3 + (u - w)^3 = 2u(u^2 + 3w^2)$.

Problem 3.

Prove that u and w are relatively prime to each other, and that exactly one of them is odd.

Case 1.

Suppose u is not divisible by 3. Then u and $3w$ are relatively prime to each other.

Problem 4.

Prove that $2u$ and u^2+3w^2 are relatively prime to each other.

It follows that there exist integers r and s such that $2u = r^3$ and $u^2+3w^2 = s^3$. We shall continue the analysis in Part Four.

Case 2.

Suppose u is divisible by 3. Then $u = 3v$ for some integer v, and $z^3 = 18v(3v^2+w^2)$.

Problem 5.

Prove that $3v$ and w are relatively prime to each other, as are $18v$ and $3v^2+w^2$.

It follows that there exist integers r and s such that $18v = r^3$ and $3v^2+w^2 = s^3$. We shall continue the analysis in Part Four.

Part Two.

Both cases in Part One lead us to consider the Diophantine equation $a^2+3b^2 = s^3$ where $(a,3b)=1$ and $a+b \equiv 1 \pmod 2$. We first explore the case where s is a prime.

Problem 6.

Prove that $s > 3$ and that neither a nor b is divisible by s.

Let b^{-1} be the inverse of b modulo s and let $g = ab^{-1}$. From $a^2+3b^2 \equiv 0 \pmod s$, we have $g^2+3 \equiv 0 \pmod s$. Let $q = \lfloor\sqrt{s}\rfloor$. Then $q < \sqrt{s} < q+1$.

Problem 7.

Prove that $g(i'-i'') \equiv j'-j'' \pmod s$ for some i', j', i'' and j'', each an integer between 0 and q inclusive, such that $(i',j') \neq (i'',j'')$.

Define $i = |i'-i''|$ and $j = |j'-j''|$. Then either $gi+j \equiv 0 \pmod s$ or $gi-j \equiv 0 \pmod s$. In any case, $g^2i^2-j^2 \equiv 0 \pmod s$.

Problem 8.

Prove that $0 < i < \sqrt{s}$ and $0 < j < \sqrt{s}$.

From $g^2+3 \equiv 0 \pmod s$, we have $g^2i^2+3i^2 \equiv 0 \pmod s$. Hence, $3i^2+j^2 \equiv 0 \pmod s$, so that $3i^2+j^2 = hs$ for some integer h.

Problem 9.

Prove that $h = 1$ or 3.

If $h=1$, then we have $s = 3i^2+j^2$. If $h=3$, then 3 divides j also, so that $j = 3k$ for some integer k. We then have $s = i^2+3k^2$. In summary, we have $s = m^2+3n^2$ for some integers m and n.

Problem 10.

Prove that $(m,3n)=1$ and $m+n \equiv 1 \pmod 2$.

We have $a^2+3b^2 = s^3 = (m^2+3n^2)^3 = m^6+9m^4n^2+27m^2n^4+27n^6$. We may take $a = m^3-Amn^2$ and $b = Bm^2n-3n^3$, so that $a^2+3b^2 = m^6+(3B^2-2A)m^4n^2+(A^2-18B)m^2n^4+27n^6$.

Problem 11.

Prove that the system of equations $3B^2 - 2A = 9$ and $A^2 - 18B = 27$ has two solutions, namely, $(A, B) = (-3, -1)$ and $(9, 3)$.

Since in Part One we attempt to find a solution smaller than the minimal solution, we take $a = m^3 - 9mn^2$ and $b = 3m^2n - 3n^3$.

Part Three.

From our exploration in Part Two, we claim that $a^2 + 3b^2 = s^3$, with $(a, 3b) = 1$ and $a + b \equiv 1 \pmod 2$, has a solution given by $s = m^2 + 3n^2$, $a = m^3 - 9mn^2$ and $b = 3m^2n - 3n^3$ for some integers m and n such that $(m, 3n) = 1$ and $m + n \equiv 1 \pmod 2$. We shall justify the claim using induction on the number ℓ of prime factors of s.

Problem 12.

Prove the claim for the case $\ell = 0$.

We could also have used the case $\ell = 1$ as the basis of our induction. Consider now the case where s has $\ell + 1$ prime factors. Let p be one of them. Then $s = tp$ where t has ℓ prime factors.

We have $a^2 + 3b^2 = s^3$, so that $a^2 + 3b^2 \equiv 0 \pmod p$. From Part Two, there exist integers c and d such that $p^3 = c^2 + 3d^2$. Moreover, $p = m_1^2 + 3n_1^2$, $c = m_1^3 - 9m_1n_1^2$ and $d = 3m_1^2n_1 - 3n_1^3$ where m_1 and n_1 are integers such that $(m_1, 3n_1) = 1$ and $m_1 + n_1 \equiv 1 \pmod 2$. Now,

$$\begin{aligned} t^3p^6 &= (a^2 + 3b^2)(c^2 + 3d^2) = (ac + 3bd)^2 + 3(ad - bc)^2 \\ &= (ac - 3bd)^2 + 3(ad + bc)^2 . \end{aligned}$$

Problem 13.

Prove that $(ad+bc)(ad-bc) = p^3(t^3d^2 - b^2)$ and deduce that p divides exactly one of $ad + bc$ and $ad - bc$.

We may assume that p divides $ad - bc$ but not $ad + bc$, since the other case can be handled in an analogous manner.

Problem 14.

Prove that p^3 divides $ad - bc$ as well as $ac + 3bd$.

Let $e = (ac + 3bd)/p^3$ and $f = (ad - bc)/p^3$.

Problem 15.

Prove that $e^2 + 3f^2 = t^3$, $a = ce + 3df$ and $b = de - cf$, and deduce that $(e, 3f) = 1$ and $e + f \equiv 1 \pmod 2$.

By the induction hypothesis, there exist integers m_2 and n_2 such that $(m_2, 3n_2) = 1$, $m_2 + n_2 \equiv 1 \pmod 2$, $t = m_2^2 + 3n_2^2$, $e = m_2^3 - 9m_2n_2^2$ and $f = 3m_2^2n_2 - 3n_2^3$. Let $m = m_1m_2 + 3n_1n_2$ and $n = m_2n_1 - n_2m_1$.

Problem 16.

Prove that $(m, 3n) = 1$, $m + n \equiv 1 \pmod 2$, $s = m^2 + 3n^2$, $a = m^3 - 9mn^2$ and $b = 3m^2n - 3n^3$.

This completes the induction argument and justifies the claim.

Part Four.

We now complete the analysis begun in Part One.

Case 1.

The equation $u^2 + 3w^2 = s^3$ has a solution in which $u = m^3 - 9mn^2$ for some integers m and n such that $(m, n) = 1$ and $m + n \equiv 1 \pmod 2$. Then $r^3 = 2u = 2m(m - 3n)(m + 3n)$.

Problem 17.

Prove that $2m$, $m - 3n$ and $m + 3n$ are pairwise relatively prime to one another.

It follows that $2m = \alpha^3$, $m - 3n = \beta^3$ and $m + 3n = \gamma^3$ for some integers α, β and γ.

Problem 18.

Prove that $\alpha^3 = \beta^3 + \gamma^3$ and $0 < |\alpha\beta\gamma| < |xyz|$.

This is the desired contradiction.

Case 2.

The equation $3v^2 + w^2 = s^3$ has a solution in which $v = m^2n - 3n^3$ for some integers m and n such that $(m, n) = 1$ and $m + n \equiv 1 \pmod 2$. Then $r^3 = 18v = 3^3(2n)(m - n)(m + n)$.

Problem 19.

Prove that $2n$, $m - n$ and $m + n$ are pairwise relatively prime to one another.

It follows that $2n = \alpha^3$, $m - n = \beta^3$ and $m + n = \gamma^3$ for some integers α, β and γ.

Problem 20.

Prove that $\alpha^3 = \beta^3 + \gamma^3$ and $0 < |\alpha\beta\gamma| < |xyz|$.

This is the desired contradiction.

Bibliography.

[1] W. Sierpinski, *Elementary Theory of Numbers*, North-Holland, Amsterdam (1988) pp. 30 and 415–418.

[2] R. Vakil, *A Do-It-Yourself Proof of the $n = 3$ case of Fermat's Last Theorem*, CRUX with MAYHEM **26** (2000) pp. 36–44.

Andy Liu
Department of Mathematical Sciences
University of Alberta
Edmonton, Alberta T6G 2G1
aliu@vega.math.ualberta.ca

An Interesting Application of the Sophie Germain Identity

Carl Johan Ragnarsson

Abstract

The readers of this article should be familiar with modular arithmetic, and may also recall Sophie Germain's identity. This article deals with an application of the identity in solving the equation $3^x + 4^y = 5^z$.

A word about the identity

As the name says, Sophie Germain's identity was first discovered by Sophie Germain. It reads

$$\begin{aligned} a^4 + 4b^4 &= a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - 4a^2b^2 \\ &= (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)\,. \end{aligned}$$

What is interesting about this identity is that sums of even powers do not generally factor. Further, such sums factor only when the term we complete the square with is, in itself, a perfect square. Its main application in contest problem solving has, so far, often been trivial because of everyone knowing the identity. When starting to read the chapter about number theory in [1], I found that the identity was used in solving some simple problems related to factoring integers, and the result was an immediate consequence of it. At the time, I was quite sure that whenever I saw another problem involving the identity, I would solve it immediately. I was totally wrong! We present here an interesting application of the identity which is by no means obvious!

The problem

We propose the following problem, which was on the IMO Short List as late as 1991, and which also appears with this source in [2].

Problem. Solve $3^x + 4^y = 5^z$ in non-negative integers.

It is natural to try to prove that the only solutions are the well-known triple $(2, 2, 2)$ and the trivial $(0, 1, 1)$. After starting to try to prove this, one may always change one's course if an obstacle is found.

Counting modulo 4, we have $(-1)^x \equiv 1 \pmod 4$, so that x is even. Let $x = 2n$, so that $9^n + 4^y = 5^z$. Now, counting modulo 5, we get $(-1)^n + (-1)^y \equiv 0 \pmod 5$, since $z \geq 1$, showing that n and y have opposite parities. We split into two cases:

Case 1: n even and y odd. Let $n = 2m$ and $y = 2t + 1$, giving that $9^{2m} + 4^{2t+1} = 5^z$, or, by application of Sophie Germain's identity,

$$\begin{aligned} & (3^m)^4 + 4 \times (2^t)^4 \\ &= \left[(3^m)^2 + 2 \times 3^m 2^t + 2 \times (2^t)^2\right] \left[(3^m)^2 - 2 \times 3^m 2^t + 2 \times (2^t)^2\right] \\ &= 5^z \,. \end{aligned}$$

Noting that the difference between the two factors is $3^m 2^{t+2}$, which is not divisible by 5, we conclude that both brackets are not multiples of 5. This implies

$$(3^m)^2 - 2 \times 3^m 2^t + 2 \times (2^t)^2 \;=\; (3^m - 2^t)^2 + (2^t)^2 \;=\; 1\,,$$

and since the two squares sum up to 1, they are 0 and 1 respectively, with $m = 0$ and $t = 0$ as the only solution. Tracing back, we easily see that this yields the triple $(0, 1, 1)$ in the original equation.

Case 2: n odd and y even. Now, similarly to Case 1, letting $y = 2t$, the equation becomes $9^n + 16^t = 5^z$. Now, counting modulo 8, we get $1 \equiv 5^z \pmod 8$, and thus, z is even. Thus, letting $z = 2w$, we obtain that $9^n + 16^t = 25^w$, or equivalently

$$(5^w)^2 - (4^t)^2 \;=\; (5^w + 4^t)(5^w - 4^t) \;=\; 3^{2n}\,,$$

and since the difference between the brackets is 2^{2t+1}, which is not divisible by 3, we conclude that $5^w - 4^t = 1$, or $5^w = 4^t + 1$. Again, counting modulo 5, we have $0 \equiv (-1)^t + 1 \pmod 5$, and thus, t is odd. Now, letting $t = 2s + 1$, we get, by a second application of Sophie Germain's identity,

$$\begin{aligned} 1 + 4^{2s+1} &= 1 + 4 \times (2^s)^4 \\ &= \left[1 + 2 \times 2^s + 2 \times (2^s)^2\right] \left[1 - 2 \times 2^s + 2 \times (2^s)^2\right] \\ &= 5^w \,. \end{aligned}$$

Finally, since the difference between the two brackets in the expression above, 2^{s+2}, is not divisible by 5, we conclude that

$$1 - 2 \times 2^s + 2 \times (2^s)^2 \;=\; (1 - 2^s)^2 + (2^s)^2 \;=\; 1\,,$$

and further, that $s = 0$. Tracing back, we easily see that this case leads back to a unique triple as well, namely $(2, 2, 2)$.

Summing up, we conclude that the equation has in all, only the two solutions $(0, 1, 1)$ and $(2, 2, 2)$.

It is interesting how much we have learned from solving this problem. Not least, it uses only the least bit of elementary number theory. It is interesting to note that once again, the triple $(3, 4, 5)$, which has appeared so many times, appears here again, and allows for some interesting problem solving methods. This also allows for brushing up some classics using the same concepts, as seen above.

Further investigation

1. Find another solution of the proposed problem!
2. For which positive integers m, n can we factor $ma^k + nb^k$?
3. In the reals, solve the system

$$\begin{aligned} 3^x + 4^y &= 5^z\,, \\ 3^y + 4^z &= 5^x\,, \\ 3^z + 4^x &= 5^y\,. \end{aligned}$$

4. Prove that for $n \geq 2$, $n^4 + 4^n$ is composite.

References

[1] Arthur Engel, *Problem Solving Strategies*, New York: Springer, 1998.
[2] Naoki Sato, *Number Theory* (unpublished).

Carl Johan Ragnarsson
Paalsjoevaegen 16 SE–223 63 Lund
Sweden
cjr2000@telia.com