Mathematical Excalibur

Volume 2, Number 3 May-June, 1996

Olympiad Corner

1996 Canadian Mathematical Olympiad:

Problem 1. If α, β and γ are the roots of $x^3 - x - 1 = 0$, compute

$$\frac{1+\alpha}{1-\alpha}+\frac{1+\beta}{1-\beta}+\frac{1+\gamma}{1-\gamma}.$$

Problem 2. Find all real solutions to the following system of equations:

$$\begin{cases} \dfrac{4x^2}{1+4x^2} = y, \\ \dfrac{4y^2}{1+4y^2} = z, \\ \dfrac{4z^2}{1+4z^2} = x. \end{cases}$$

Carefully justify your answer.

Problem 3. We denote an arbitrary permutation of the integers 1, 2, ⋯, n by $a_1, a_2, \cdots, a_n$. Let $f(n)$ be the number of these permutations such that

(i) $a_1 = 1$;

(*continued on page 4*)

The editors welcome contributions from all teachers and students. With your submission, please include your name, address, school, email, telephone and fax numbers (if available). Electronic submissions, especially in MS Word are encouraged. The deadline for receiving material for the next issue is July 10, 1996.

For individual subscription for the five issues for the 96-97 academic year, send us five stamped self-addressed envelope. Send all correspondence to:

Dr. Kin-Yin Li
Department of Mathematics
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong

Fax: 2358-1643
Email: makyli@uxmail.ust.hk

Fermat's Little Theorem and Other Stories

T.W. Leung
Hong Kong Polytechnic University

Pierre de Fermat (1601-1665), a councilor of the provincial High Court of Judicature in Toulouse, south of France, practised mathematics during his spare time. He discussed his findings with his friends via letters. As it turned out, his works significantly influenced the development of modern mathematics. During Fermat's time, the following "Chinese hypothesis" was around:

p is a prime if and only if $2^p \equiv 2 \pmod p$.

One direction of the hypothesis is not true. In fact $2^{341} - 2$ is divisible by 341, yet 341 = 11 × 31 is composite (not prime). However the other direction is indeed valid. From the manuscripts and letters of Fermat, we conclude that Fermat knew (and most likely could prove) the following facts:

(1) If n is not a prime, then $2^n - 1$ is not a prime.
(2) If n is a prime, then $2^n - 2$ is a multiple of $2n$.
(3) If n is a prime, and p is a prime divisor of $2^n - 1$, then $p - 1$ is a multiple of n.

The first statement can be proved directly by factoring $2^n - 1$. If $n = pq$ (with $p > 1$ and $q > 1$), then

$$\begin{aligned} 2^n - 1 &= 2^{pq} - 1 \\ &= (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \cdots + 1). \end{aligned}$$

The other two statements are variations of the more general statement, indicated in his other letter:

> Given any prime p, and any geometric progression 1, a, a^2, ⋯, the number p must divide some number $a^n - 1$, for which n divides $p-1$; if then N is any multiple of the smallest number n for which this is so, p divides also $a^N - 1$.

With modern mathematical notation, we may rewrite Fermat's statement as the following which will be referred to as Fermat's Little Theorem:

> If p is a prime number and a is any integer, then $a^p \equiv a \pmod p$. In particular, if p does not divide a, then $a^{p-1} \equiv 1 \pmod p$.

Now we see how Fermat made use of his little theorem. He was challenged to determine if there is any even perfect number lying between 10^{20} and 10^{22}. (A positive integer n is called a perfect number if the sum of all proper factors (i.e., excluding n) of n is equal to n. For example, $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$ are perfect numbers.) This problem can be reduced (how?) to check if $2^{37} - 1$ is prime. Suppose the number is not prime, and p is an odd prime divisor of that number, then from the third statement, $p - 1$ is a multiple of 37, or $p = 37k + 1$, observe that p is odd, so k is even, or p is of the form $74k' + 1$. The first few candidates are 149, 223, ⋯. One then check that

$$\begin{aligned} 2^{37} - 1 &= 137438953471 \\ &= 223 \times 616318177. \end{aligned}$$

It is more difficult to check that the second factor is a prime, however Fermat succeeded in showing that $2^{37} - 1$ is not prime.

Another side story comes from the fact that if $2^m + 1$ is prime, then m must be of the form 2^n. Fermat conjectured that all these numbers are prime. Now $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$ and $2^{2^4} + 1 = 65537$ are indeed prime numbers. However,

$$2^{2^5} + 1 = 4294967297$$

is not a prime. In fact, if p is a prime factor of $2^{2^n} + 1$, then 2^{n+1} is the smallest

(*continued on page 2*)

Fermat's Little Theorem ...

(*continued from page 1*)

m satisfying $2^m \equiv 1 \pmod p$, thus 2^{n+1} divides $p-1$, or p is of the form $k2^{n+1}+1$, hence to look for prime factors of $2^{2^5}+1 = 2^{32}+1$, we should consider primes of the form $64k+1$. The possible candidates are 193, 257, 449, 577, 641, $\cdots$. Unfortunately, neither Fermat nor his contemporaries had enough patience to check that 641 indeed divides $2^{32}+1$. (For readers who are familiar with the law of quadratic reciprocity, one can prove that a prime divisor of $2^{2^n}+1$ is actually of the form $k2^{n+2}+1$.)

Fermat did not explicitly give any proof of the Fermat's little theorem, and it was Euler who first proved by induction the following fact: if p is a prime then $a^p \equiv a \pmod p$. Clearly the statement is true if $a = 1$. Now

$$(a+1)^p \equiv a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + 1 \equiv a+1 \pmod p,$$

where $\binom{p}{i} = \dfrac{p!}{i!(p-i)!} \equiv 0 \pmod p$ for $1 \le i \le p-1$.

There is also another version of the theorem, namely, if p is a prime and a is relatively prime to p, then $a^{p-1} \equiv 1 \pmod p$. Euler also gave the first proof by noting that the terms of the series $1, a, a^2, \cdots \pmod p$ must repeat. So for some $r \ge 0$, and some $s \ge 0$, we must have $a^{r+s} \equiv a^r \pmod p$, i.e., $a^s \equiv 1 \pmod p$. Let s be the smallest positive integer such that $a^s \equiv 1 \pmod p$, then one can arrange the $p-1$ non-zero congruence classes modulo p into sets $\{b, ba, \cdots, ba^{s-1}\}$, where each set consists of s elements and the sets are disjoint. Thus s must divide $p-1$. For example, with $p = 7$ and $a = 2$, one obtains $s = 3$ and the numbers 1 to 6 can be grouped into two disjoint sets $\{1, 2, 4\}$ and $\{3, 6, 5\}$. We also observe that $p-1 = 6$ is divisible by $s = 3$. Euler generalized this argument to prove the famous Euler's theorem:

If a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod n$,

where $\phi(n)$ is the Euler totient function that counts the number of integers between 1 and n that are relatively prime to n. For example, $\phi(12) = 4$ since only 1, 5, 7, 11 (among the numbers 1-12) are relatively prime to 12.

A formal proof of Euler's theorem goes as follows: Let a be an integer relatively prime to n and let $\{a_1, a_2, \ldots, a_{\phi(n)}\}$ be the set of reduced residues modulo n (i.e., the $\phi(n)$ positive integers less than n that are relatively prime to n). Then the set $\{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$ is also a set of reduced residues modulo n. Hence,

$$a_1a_2\cdots a_{\phi(n)} \equiv a^{\phi(n)}a_1a_2\cdots a_{\phi(n)} \pmod n$$

or $$a^{\phi(n)} \equiv 1 \pmod n.$$

There is however another colouring argument for Fermat's little theorem. Arrange p boxes in a circle and colour them with a colours. There are a^p possible colouring patterns. Among all these possible colourings, a of them are such that every box has the same colour. The remaining $a^p - a$ colouring patterns can be grouped into sets of p patterns that are rotations of each other. The p rotations of any one of these colourings are all distinct and thus p divides $a^p - a$. (Where did we use "p is prime"?) Hence, in essence, the Fermat's little theorem can be proved using the pigeonhole principle.

The following are some applications of Fermat's little theorem and Euler's theorem.

Example 1: If n is an integer > 1, then n does not divide $2^n - 1$.

Solution: If n is even, then the statement is certainly true since $2^n - 1$ is an odd integer. For n odd, denote by p the smallest prime divisor of n. Suppose n (and thus also p) divides $2^n - 1$. By the Fermat's little theorem, p divides $2^{p-1} - 1$ too. Consequently, p divides $2^d - 1$, where d is the greatest common divisor of $p-1$ and n, Since p is the smallest prime divisor of n, $d = 1$ which leads to the contradiction p divides 1.

Example 2: Let n be an odd number not divisible by 5, then n divides a number of the form $99\cdots9$.

Solution: If n is odd and not divisible by 5, then n is relatively prime to 10. By the Euler's theorem, $10^{\phi(n)} \equiv 1 \pmod n$, i.e., n divides $10^{\phi(n)} - 1$, which is a number of the form $99\cdots9$.

Example 3: Let p be an odd prime number. Then for any set of $2p-1$ integers, there exists a set of p integers whose sum is divisible by p.

Sketch of Solution: There are $n = \binom{2p-1}{p}$ distinct sets that each contains p elements. Denote their sums by $s_1, s_2, \ldots, s_n$. Suppose none of them is divisible by p. Then, by the Fermat's little theorem, $\sum_{i=1}^{n} s_i^{p-1} = \sum_{i=1}^{n} 1 = n$, which is nonzero modulo p. On the other hand, one may use the multinomial expansion to show that $\sum_{i=1}^{n} s_i^{p-1}$ is, in fact, divisible by p, and thus lead to a contradiction.

It is interesting to observe that we use a number theoretic approach to solve a combinatorial problem while using a counting argument to prove Fermat's little theorem.

We have mentioned that the converse of Fermat's little theorem is not true. That is, there exists composite numbers n such that n divides $a^{n-1} - 1$. For example, as stated at the beginning of this article, the composite number 341 divides $2^{340} - 1$. Composite numbers n (which must be odd) that divides $2^{n-1} - 1$ are called pseudoprimes (in base 2). One may show that there exist infinitely many such pseudoprimes. In fact, if n is a pseudoprime, then $m = 2^n - 1$ will be composite (since n is composite). Also, $m - 1 = 2^n - 2 = nk$ and thus $2^{m-1} - 1 = 2^{nk} - 1$ is divisible by $2^n - 1 = m$. That is, m is another pseudoprime (in base 2).

We may of course try another base. For our example, we find that 341 is no longer a pseudoprime (in base 3), i.e., 341 does not divide $3^{340} - 1$. Well, we may then ask: is it possible to find a composite number n such that for every a relatively prime to n, $a^{n-1} \equiv 1 \pmod n$. Such a number is called a Carmichael number. Surprisingly, not only that they exist (with 561 being the smallest), there are infinitely many Carmichael numbers, which, in fact, was proved recently!

Problem Corner

We welcome readers to submit solutions to the problems posed below for publication consideration. Solutions should be preceded by the solver's name, address, school affiliation and grade level. Please send submissions to *Dr. Kin-Yin Li, Dept of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon.* The deadline for submitting solutions is July 10, 1996.

The following problems are selected from the International Mathematics Tournament of the Towns, held in April 7, 1996.

Problem 36. Let a, b and c be positive numbers such that $a^2 + b^2 - ab = c^2$. Prove that $(a-c)(b-c) \le 0$.

Problem 37. Two non-intersecting circles λ_1 and λ_2 have centres O_1 and O_2 respectively. A_1 and A_2 are points on λ_1 and λ_2 respectively, such that A_1A_2 is an external common tangent of the circles. The segment O_1O_2 intersects λ_1 and λ_2 at B_1 and B_2 respectively. The lines A_1B_1 and A_2B_2 intersect at C, and the line through C perpendicular to B_1B_2 intersects A_1A_2 at D. Prove that D is the midpoint of A_1A_2.

Problem 38. Prove that from any sequence of 1996 real numbers, one can choose a block of consecutive terms whose sum differs from an integer by at most 0.001.

Problem 39. Eight students took part in a contest with eight problems.

(a) Each problem was solved by 5 students. Prove that there were two students who between them solved all eight problems.

(b) Prove that this is not necessarily the case if 5 is replaced by 4. (A counterexample is enough.)

Problem 40. ABC is an equilateral triangle. For a positive integer $n \ge 2$, D is the point on AB such that $AD = \frac{1}{n}AB$. $P_1, P_2, \cdots, P_{n-1}$ are points on BC which divide it into n equal segments. Prove that $\angle AP_1D + \angle AP_2D + \cdots + \angle AP_{n-1}D = 30°$.

[*Hint*: Consider Q_i such that ADP_iQ_i is a parallelogram.]

****

Solutions

****

Problem 31. Show that for any three given odd integers, there is an odd integer such that the sum of the squares of these four integers is also a square.

Solution: Independent solution by **William CHEUNG Pok-man** (S.T.F.A. Leung Kau Kui College, Form 5), **Gary NG Ka Wing** (S.T.F.A. Leung Kau Kui College, Form 3), **Henry NG Ka Man** (S.T.F.A. Leung Kau Kui College, Form 5) and **PAI Hung Ming Tedward** (S.K.H. Tang Shiu Kin Secondary School, Form 6).

Let $x = 2a + 1, y = 2b + 1, z = 2c + 1$ be three given odd integers, then $x^2 + y^2 + z^2 = 2w + 1$, where $w = 2(a^2 + a + b^2 + b + c^2 + c) + 1$ is odd. So $x^2 + y^2 + z^2 + w^2 = (w + 1)^2$.

Other commended solver: **CHAN Wing Chiu** (La Salle College, Form 3), **CHENG Wing Kin** (S.K.H. Lam Woo Secondary School, Form 4), **Calvin CHEUNG Cheuk Lun** (S.T.F.A. Leung Kau Kui College, Form 4), **W. H. FOK** (Homantin Government Secondary School), **Alan LEUNG Wing Lun** (S.T.F.A. Leung Kau Kui College, Form 4), **LIU Wai Kwong** (Pui Tak Canossian College), **POON Wing Chi** (La Salle College) and **YAU Kwan Kiu** (Queen's College, Form 7).

Problem 32. Let $a_0 = 1996$ and $a_{n+1} = a_n^2/(a_n + 1)$ for $n = 0, 1, 2, \ldots$. Prove that $[a_n] = 1996 - n$ for $n = 0, 1, 2, \ldots, 999$, where $[x]$ is the greatest integer less than or equal to x.

Solution: Independent solution by **CHAN Wing Sum** (HKUST), **W. H. FOK** (Homantin Government Secondary School) and **KU Yuk Lun** (HKUST).

Note that $a_n > 0$ implies $a_{n+1} > 0$ and

$$a_n - a_{n+1} = 1 - \frac{1}{a_n + 1} > 0.$$

Hence $a_0 > a_1 > a_2 > \cdots$. Now

$$\begin{aligned} a_n &= a_0 + (a_1 - a_0) + \cdots + (a_n - a_{n-1}) \\ &= 1996 - n + \frac{1}{a_0 + 1} + \cdots + \frac{1}{a_{n-1} + 1} \\ &> 1996 - n. \end{aligned}$$

For $1 \le n \le 999$,

$$\begin{aligned} \frac{1}{a_0 + 1} + \cdots + \frac{1}{a_{n-1} + 1} &< \frac{n}{a_{n-1} + 1} \\ &< \frac{999}{a_{998} + 1} < \frac{999}{1996 - 998 + 1} = 1. \end{aligned}$$

So $[a_n] = 1996 - n$.

Comments: With 1996 replaced by 1994, 999 replaced by 998, this was a problem proposed by USA in the 1994 IMO.

Other commended solver: **William CHEUNG Pok-man** (S.T.F.A. Leung Kau Kui College, Form 5), **Henry NG Ka Man** (S.T.F.A. Leung Kau Kui College, Form 5), **POON Wing Chi** (La Salle College) and **YAU Kwan Kiu** (Queen's College, Form 7).

Problem 33. Let A, B, C be noncollinear points. Prove that there is a unique point X in the plane of ABC such that $XA^2 + XB^2 + AB^2 = XB^2 + XC^2 + BC^2 = XC^2 + XA^2 + CA^2$. (A problem proposed by Germany in the last IMO.)

Solution: Henry NG Ka Man (S.T.F.A. Leung Kau Kui College, Form 5).

Without loss of generality, we may assume A, B, C have coordinates $(a,0)$, $(b,0)$, $(0,c)$, (where $a \ne b$ and $c \ne 0$) respectively. Let X be a point in the plane of ABC with coordinates (x,y). For X to satisfy the given conditions, the equations on x and y are $ax - cy = a^2 - c^2 - ab$, $bx - cy = b^2 - c^2 - ab$ and $x = a + b$ (after simplification), which has a unique solution $(x,y) = (a+b, c+2ab/c)$.

Other commended solvers: **Calvin CHEUNG Cheuk Lun** (S.T.F.A. Leung Kau Kui College, Form 4), **William CHEUNG Pok-man** (S.T.F.A. Leung Kau Kui College, Form 5), **W. H. FOK** (Homantin Government Secondary School), **Alan LEUNG Wing Lun** (S.T.F.A. Leung Kau Kui College, Form 4), **LIU Wai Kwong** (Pui Tak Canossian College) and **Gary NG Ka Wing** (S.T.F.A. Leung Kau Kui College, Form 3).

Problem 34. Let $n > 2$ be an integer, c be a nonzero real number and z be a nonreal

(continued on page 4)

Problem Corner

(*continued from page 3*)

root of $X^n + cX + 1$. Show that

$$|z| \geq \frac{1}{\sqrt[n]{n-1}}.$$

Solution 1: W. H. FOK (Homantin Government Secondary School).

Write $z = r(\cos\theta + i\sin\theta)$ with $\sin\theta \neq 0$. Taking the real and imaginary parts of $z^n + cz + 1 = 0$ using De Moivre's theorem, we have

$$r^n\cos n\theta + cr\cos\theta + 1 = 0$$

and $$r^n\sin n\theta + cr\sin\theta = 0.$$

Then

$$\begin{aligned} r^n\sin(n-1)\theta &= r^n\sin n\theta\cos\theta - r^n\cos n\theta\sin\theta \\ &= -cr\sin\theta\cos\theta + (cr\cos\theta + 1)\sin\theta \\ &= \sin\theta. \end{aligned}$$

Since

$$\begin{aligned} |\sin(k+1)\theta| &= |\sin k\theta\cos\theta + \cos k\theta\sin\theta| \\ &\leq |\sin k\theta| + |\sin\theta|, \end{aligned}$$

induction gives $|\sin k\theta| \leq k|\sin\theta|$ for every positive integer k. So

$$|z|^n = r^n = |\sin\theta/\sin(n-1)\theta| \geq 1/(n-1).$$

Solution 2: LEUNG Hoi-Ming (SKH Lui Ming Choi Secondary School).

Let $r = |z|$ and $w = z/r$. Then $|w| = 1$ and $w\overline{w} = 1$. Since $(rw)^n + crw + 1 = 0$, multiplying by $\overline{w}$, then conjugating, we get

$$r^n w^{n-1} + cr + \overline{w} = 0$$

and $$r^n \overline{w}^{n-1} + cr + w = 0.$$

Subtracting these equations and solving for r^n, we get

$$r^n = \frac{w - \overline{w}}{w^{n-1} - \overline{w}^{n-1}} = \frac{1}{\sum_{i=0}^{n-2} w^{n-2-i}\overline{w}^i}.$$

Since r is real and $|w| = 1$, by the triangle inequality,

$$r^n \geq \frac{1}{\sum_{i=0}^{n-2} |w^{n-2-i}\overline{w}^i|} = \frac{1}{n-1}.$$

Other commended solvers: **William CHEUNG Pok-man** (S.T.F.A. Leung Kau Kui College, Form 5).

Problem 35. On a blackboard, nine 0's and one 1 are written. If any two of the numbers on the board may both be replaced by their average in one operation, what is the least *positive* number that can appear on the board after a finite number of such operations?

Solution: POON Wing Chi (La Salle College).

Let m be the least positive number on the board and n be the number of zeros on the board after an operation. Consider the number $c = m/2^n$. If two positive numbers are both replaced by their average, then n does not change, but m (and c) may increase. If a 0 is averaged with a positive number r, then n decreases by one and m remains unchanged or becomes $r/2$ ($\geq m/2$.) The new c value will be greater than or equal to $(m/2)/2^{n-1} = m/2^n$, which is the old c value. In the beginning, $c = 1/512$. After a finite number of operations, $c \geq 1/512$ and $m \geq 2^n/512 \geq 1/512$. To obtain exactly 1/512, start with 1 and average with each of the nine 0's.

Comments: This problem comes from an article in the March/April 1994 issue of *Quantum*, published by Springer Verlag. The article dealt with the concept of *monoinvariant*, which is an expression like c in the problem that increases after each operation. Studying such expression often solves the problem.

Olympiad Corner

(*continued from page 1*)

(ii) $|a_i - a_{i+1}| \leq 2, \quad i = 1, \cdots, n-1.$

Determine whether $f(1996)$ is divisible by 3.

Problem 4. In ΔABC, $AB = AC$. Suppose that the bisector of $\angle B$ meets AC at D and that $BC = BD + AD$. Determine $\angle A$.

Problem 5. Let $r_1, r_2, \ldots, r_m$ be m given positive rational numbers such that

$$\sum_{k=1}^{m} r_k = 1.$$

Define the function f by

$$f(n) = n - \sum_{k=1}^{m} \lfloor r_k n \rfloor$$

for each positive integer n. Determine the minimum and maximum values of $f(n)$.

From the Editors' Desk:

Thanks to our readers for another year of support, especially the submission of articles and problem solutions. If you would like to receive your personal copy for the five issues for the 96-97 academic year, send five stamped self-addressed envelopes to Dr. Kin-Yin Li, Hong Kong University of Science and Technology, Department of Mathematics, Clear Water Bay, Kowloon, Hong Kong.

****

APMO and **IMO**: The Eighth APMO took place on March 16th. The Hong Kong students had a very strong (record setting) performance. The top 8 scorers are as follow. (Note the maximum is 7×5=35 points.)

1. 潘維凱 (**Bobby POON Wai Hoi**), St. Paul's College, 35 points (Perfect score! First time for Hong Kong)
2. 余振陵 (**YU Chun Ling**), Ying Wa College, 33 points
3. 何穎業 (**HO Wing Yip**), Clementi Secondary School, 32 points
4. 莫子韜 (**MOK Tsz Tao**), Queen's College, 31 points
5. 謝珊珊 (**TSE Shan Shan**), Tuen Mun Government Secondary School, 29 points
6. 羅肇龍 (**LAW Siu Lung**), Diocesan Boy's School, 26 points
7. 翁漢威 (**YUNG Hon Wai**), Heep Woh College, 26 points
8. 朱天健 (**CHU Tim Kin**), King's College, 24 points

The first 6 students are invited to be the Hong Kong team members to participate in the 37th International Mathematical Olympiad to be held in India this summer. The selection was based on their outstanding performance in the APMO and throughout the Hong Kong Math Olympiad training program.