Problem 1. If $\alpha$, $\beta$ and $\gamma$ are the roots of $x^3 - x - 1 = 0$, compute

$$
\begin{align*}
1 + \alpha &= 1 + \beta + 1 + \gamma, \\
1 - \alpha &= 1 - \beta - 1 - \gamma.
\end{align*}
$$

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

$$
\begin{align*}
4x^2 &= y, \\
1 + 4x^2 &= z, \\
1 + 4y^2 &= z, \\
1 + 4z^2 &= x.
\end{align*}
$$

Carefully justify your answer.

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

$$
\begin{align*}
f_1 &= 1; \\
(continued\ on\ page\ 4)
\end{align*}
$$

Editor: Cheung, Pak-Kong, CTR, Studies, HKU
King, Ting-Mei, IEEE, Hong Kong University
Leung, Wing-Wing, Applied Math Dept., HKUST
Liu, Kin-Yin, Math Dept., HKUST
Ng, Kong Po Roger, ITC, HKUST
Artist: Yung, Siu-Ying Camille, MFA, CU

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

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

Dr. Kin-Yin Liu
Department of Mathematics
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong
Fax: 2358-1643
Email: makkyk@hotmail.net.hk

Fermat's Little Theorem and Other Stories

T.W. Leung
Hong Kong Polytechnic University

Pierre de Fermat (1601-1665), a councillor of the provincial high Court of judicature in Toulouse, south of France, prised 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:

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 was an even perfect number lying between $2^{10}$ and $2^{12}$. (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 $2^{2n} - 1$ is prime. Suppose the number is not prime, and $p$ is an odd prime divisor of $2^{2n} - 1$, then from the third statement, $p - 1$ is a multiple of 37, or $p = 37a + 1$, where $p$ is odd, so $4$ is even, or $p$ is of the form $74t + 1$. The first few candidates are 149, 223, ...

One then check that $2^{211} - 1 = 134 \times 38953471 = 223 \times 616318177$.

It is more difficult to check that the second factor is a prime, however Fermat succeeded in showing that $2^{211} - 1$ is not prime.

Another side story comes from the fact that if $2^{2n} + 1$ is prime, then $n$ must be of the form $2^m$. Fermat conjectured that all these numbers are prime. Now $2^3 + 1 = 5, 2^7 + 1 = 17, 2^{25} + 1 = 257$ and $2^{65537} + 1 = 65537$ are indeed prime numbers. However, $2^{2^3} + 1 = 249495727$ is not prime. In fact, if $p$ is a prime factor of $2^{2^n} + 1$, then $2^n$ is the smallest (continued on page 2)
Fermat's Little Theorem ...

(continued from page 1)

...satisfying $2^n \equiv 1 \pmod{p}$, thus $2^{2^n} \equiv 1 \pmod{p}$, or $p$ is of the form $2k+1$, hence to look for prime factors of $2^n + 1 = 2^{2n} + 1$, we should consider primes of the form $64k + 1$. The possible candidates are $193, 257, 449, 577, 641$. 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 $2\mid \text{divisor of } 2^{2n} + 1$ is actually of the form $2k+1$.)

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 $n^p \equiv n \pmod{p}$. Clearly the statement is true if $n = 1$. Now

$2^{2^n} \equiv 1 \pmod{p}$

...and

$2^{2^n+1} \equiv 1 \pmod{p}$

...which proves $2^{2^n+1} \equiv 1 \pmod{p}$ for $1 \leq n \leq p-1$.

There is also another version of the theorem, namely, if $p$ is a prime and $a$ is relatively prime to $p$, then $a^p \equiv a \pmod{p}$ (Euler). Euler also gave the first proof by noting that the terms of the series $1, a, a^2, \ldots \pmod{p}$ repeat. For some $x \geq 0$, and some $y \geq 0$, we must have $a^x = a^y \pmod{p}$, i.e., $a^x \equiv 1 \pmod{p}$. Let $x$ be the smallest positive integer such that $a^x \equiv 1 \pmod{p}$, then $a^x \equiv 1 \pmod{p}$, or $x = 1$. Euler generalized this argument to prove the famous Euler's theorem:

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

where $\varphi(n)$ is the Euler totient function that counts the number of integers between 1 and $n$ that are relatively prime to $n$. For example, $\varphi(12) = 4$ 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 $(a, a_n, \ldots, a_{n-1})$ be the set of reduced residues modulo $n$ (i.e., the $\mathbb{Q}$ positive integers less than $n$ that are relatively prime to $n$). Then the set $(a, a_n, a_{n-1}, \ldots, a_0)$ is also a set of reduced residues modulo $n$.

Hence,

$a_{n-1} \equiv a_{n-2} \equiv \cdots \equiv a_0 \equiv 1 \pmod{n}$

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 $a$ 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 "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 $2^{p-1} - 1$. Consequently, $p$ divides $2^n - 1$, 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 $99\cdots 9$.

**Solution:** If $n$ is odd and not divisible by 5, then $n$ is relatively prime to 10. By the Euler's theorem, $2^{\varphi(n)} \equiv 1 \pmod{n}$, i.e., $n$ divides $10^\varphi(n) - 1$, which is a number of the form $99\cdots 9$. 

**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 Proof:** There are $\frac{2p-1}{p}$ distinct sets that each contains $p$ elements. Denote their sums by $s_1, s_2, \ldots, s_{2p-1}$. Suppose none of them is divisible by $p$. Then, by the Fermat's little theorem, $\sum_{i=1}^{2p-1} s_i = 0$, which is nonzero modulo $p$. On the other hand, one may use the multinomial expansion to show that $\sum_{i=1}^{2p-1} s_i$ 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 such that $n$ divides $a^n - 1$. 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 $2^n - 1$ are called pseudoprimes (in base 2). One may show that there exist infinitely many such pseudoprimes. In fact, if $n$ is a pseudoprime, then $n - 2^k - 1$ will be composite (since $n$ is composite). Also, $n - 1 = 2^k - 2$ and $n = 2^k - 2$ and $2^n - 1$ is divisible by $2^n - 1 = m$. That is, $m$ is another pseudoprime (in base 2).

We may choose our base case for our example. For our base, 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 such that for every $a$ relatively prime to $n$, $a^{340} \equiv 1 \pmod{n}$. 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, were 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 and 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 4, 1996.

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

Problem 37. Two non-intersecting circles \(A_1\) and \(A_2\) have centres \(O_1\) and \(O_2\) respectively, and \(A_1A_2\) is a point on \(A_1\) and \(A_2\) respectively, such that \(A_1A_2\) is an external common tangent of the circles. The segment \(O_1A_2\) intersects \(A_1A_2\) 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 content 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. In a triangle, \(a\), \(b\), and \(c\) are sides and \(\alpha\), \(\beta\), and \(\gamma\) are the opposite angles. Prove that \(\sin \alpha \cdot \sin \beta \cdot \sin \gamma = \frac{a \cdot b \cdot c}{4abc}\). (HINT: Consider \(\frac{a \cdot b \cdot c}{4\sin \alpha \cdot \sin \beta \cdot \sin \gamma}\) which is a parallelogram.)

Solutions

Problem 36. 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 an integer.


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

Other commented solver: CHAN Wing Chiu (La Salle College, Form 3), CHENG Wing Kin (S.K.H. Luns Waa Secondary School, Form 4), Calvin CHEUNG Cheuk Lun (S.T.F.A. Leung Kau Kui College, Form 4), POON Wing Chi (La Salle College) and YAU Kwun Kiu (Queen’s College, Form 7).

Problem 37. Let \(a_1, a_2, \ldots, a_n\) be nonnegative numbers. Prove that \(a_1 \geq a_2 \geq \cdots \geq a_n\).


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

Problem 38. Without loss of generality, we may assume \(A, B, C\) are co-ordinates \((a_0, b), (b_0, 0), (c_0, 0)\) respectively. Let \(X = 2z\) be a point in the plane of \(ABC\) with co-ordinates \((x, y)\). For \(z\) to satisfy the given conditions, the equations \(ax + by = c_0 \pm ab\), \(bx - cy = a_0 \pm ab\) and \(x = x + 1\) (after simplification), which has a unique solution \((x, y) = (a_0b + c_0ab, c_0b + a_0ab)\).

Other commented solver: 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 1), Calvin CHEUNG Cheuk Lun (S.T.F.A. Leung Kau Kui College, Form 3), LIU Wai Kwong (Pui Tak Canossian College) and Gary NG Ka Wing (S.T.F.A. Leung Kau Kui College, Form 3).

Problem 39. Let \(n \geq 2\) 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 $x^2 + cx + 1 = 0$. Show that

$$|\alpha| > \sqrt{n} - 1$$


Write $z = r \cos \theta + i \sin \theta$ with $|z| \neq 0$.

Taking the real and imaginary parts of $z^2 + cz + 1 = 0$ using De Moivre's theorem, we have

\[ r^2 \cos 2\theta + r \cos \theta = 1 \quad \text{and} \quad r^2 \sin 2\theta + r \sin \theta = 0. \]

Then

\[ r^2 \sin (n-1)\theta = r \sin \theta \cos (n-1)\theta - r \cos \theta \sin (n-1)\theta = -r \sin \theta \cos \theta + r \cos \theta \sin \theta = 0. \]

Since

\[ |\sin (n+1)\theta| = |\sin \theta \cos (n-1)\theta| \leq |\sin \theta| \leq |\sin \theta| \quad \text{for every positive integer} \quad n, \]

we have

\[ |\sin (n+1)\theta| = \frac{r^2 \sin (n-1)\theta}{r \cos \theta} \geq \frac{1}{1/(k-1)}. \]

Solution 2: LEUNG Hoi-Ming (SKH Lai Ming Choy Secondary School).

Let $r = \frac{1}{w}$ and $w = \frac{1}{z}$. Then $|w| = 1$ and $w^2 = w$. Since $(cw) + c + 1 = 0$, multiplying by $w$, we get

\[ r^2 - w^2 + cr + w = 0 \quad \text{and} \quad r^2 w^2 + cw + w = 0. \]

Subtracting these equations and solving for $r$, we get

\[ r^2 - w^2 - w = 1 + \sum_{i=0}^{n-2} w^{2i} \]

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

\[ r^2 \geq \frac{1}{\sum_{i=0}^{n-2} w^{2i}} = \frac{1}{n-1}. \]

Other commendable solvers: WILLIAM CHEUNG Pok-man (S.T.F.A. Leung Kaw Kui College, Form 5).

Problem 35. On a blackboard, nine $\frac{9}{11}$ and one $\frac{1}{1}$ are written. If any two of the numbers on the blackboard 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 $n$ be the least positive number on the board and $m$ be the number of zeros on the board after an operation. Consider the number $c = m^2 - n^2$. If two positive numbers are both replaced by their average, then $m$ does not change, but $n$ may increase. If $0$ is averaged with a positive number $r$, then $n$ decreases by one and $m$ remains unchanged or becomes $m^2/2$. The number $c$ will be greater than or equal to $(m^2/2)^2 - n^2$, which is the old value $c$. In the beginning, $c = 1/512$. After a finite number of operations, $c \geq 1/512$ and $m \geq 20/512 \geq 1/512$. 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 Quaestiones, published by Springer Verlag. The article deals with the concept of minimax, 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) $|a_i - a_{i+1}| \leq 1, \quad i = 1, \ldots, n-1.$

Define the function $f$ by

\[ f(n) = n - \sum_{k=1}^{n} |a_k| \]

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-Yat 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 follows. (Note the maximum is 7×5=35 points.)

1. 潘志明 (Bobby POON Wai Hoi), St. Paul’s College, 35 points (Perfect score! First time for Hong Kong).
2. 余振煜 (YU Chun Lung), Ying Wa College, 33 points
3. 何嘉樂 (HO Wung Yip), Clementi Secondary School, 32 points
4. 朱子健 (MOH Tsu Tung), Queen’s College, 31 points
5. 謝德輝 (TSE Shan Shan), Tsuen Wan Government Secondary School, 30 points
6. 羅嘉龍 (LAW Siu Lung), Diocesan Boys’ School, 26 points
7. 崔堅 (YUNG Hon Wai), Heep Woh College, 26 points
8. 朱天健 (CHU Tsz Kin), King’s College, 24 points

The first 6 students are invited to be the Hong Kong team members to participate in the 57th 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.