Mathematical Excalibur

Volume 15, Number 1 *May 2010-June, 2010*

Olympiad Corner

Below are the First Round problems of the 26th Iranian Math Olympiad.

Problem 1. In how many ways can one choose $n-3$ diagonals of a regular n-gon, so that no two have an intersection strictly inside the n-gon, and no three form a triangle?

Problem 2. Let ABC be a triangle. Let I_a be the center of its A-excircle. Assume that the A-excircle touches AB and AC in B' and C', respectively. Let I_aB and I_aC intersect $B'C'$ in P and Q, respectively. Let M be the intersection of CP and BQ. Prove that the distance between M and the line BC is equal to the inradius of ΔABC.

Problem 3. Let a, b, c and d be real numbers, and at least one of c or d is not zero. Let $f:\mathbb{R}\to\mathbb{R}$ be the function defined by

$$f(x)=\frac{ax+b}{cx+d}.$$

Assume that $f(x)\neq x$ for every $x\in\mathbb{R}$. Prove that there exists at least one p such that $f^{1387}(p)=p$, then for every x, for which $f^{1387}(x)$ is defined, we have $f^{1387}(x)=x$.

(continued on page 4)

Acknowledgment: Thanks to Elina Chiu, Math. Dept., HKUST for general assistance.

On-line:
http://www.math.ust.hk/mathematical_excalibur/

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, 2010***.

For individual subscription for the next five issues for the 09-10 academic year, send us five stamped self-addressed envelopes. Send all correspondence to:

Dr. Kin-Yin LI, Math Dept., Hong Kong Univ. of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

Fax: (852) 2358 1643
Email: makyli@ust.hk

Primitive Roots Modulo Primes

Kin Y. Li

The well-known Fermat's little theorem asserts that if p is a prime number and x is an integer not divisible by p, then

$$x^{p-1}\equiv 1 \pmod p.$$

For positive integer $n>1$ and integer x, if there exists a least positive integer d such that $x^d\equiv 1 \pmod n$, then we say d is the *order* of x (mod n). We denote this by $ord_n(x)=d$. It is natural to ask for a prime p, if there exists x such that $ord_p(x)=p-1$. Such x is called a *primitive root (mod p)*. Indeed, we have the following

Theorem. For every prime number p, there exists a primitive root (mod p). (We will comment on the proof at the end of the article.)

As a consequence, if x is a primitive root (mod p), then $1, x, x^2, \ldots, x^{p-2} \pmod p$ are distinct and they form a permutation of $1, 2, \ldots, p-1 \pmod p$. This is useful in solving some problems in math competitions. The following are some examples. (Below, we will use the common notation $a|b$ to denote a is a divisor of b.)

Example 1. (*2009 Hungary-Israel Math Competition*) Let $p\geq 2$ be a prime number. Determine all positive integers k such that $S_k=1^k+2^k+\cdots+(p-1)^k$ is divisible by p.

Solution. Let x be a primitive root (mod p). Then

$$S_k\equiv 1+x^k+\cdots+x^{(p-2)k} \pmod p.$$

If $p-1\,|\,k$, then $S_k\equiv 1+\cdots+1=p-1 \pmod p$. If $p-1\nmid k$, then since $x^k\not\equiv 1 \pmod p$ and $x^{(p-1)k}\equiv 1 \pmod p$, we have

$$S_k\equiv\frac{x^{(p-1)k}-1}{x^k-1}\equiv 0 \pmod p.$$

Therefore, all the k's that satisfy the requirement are precisely those integers that are not divisible by $p-1$.

Example 2. Prove that if p is a prime number, then $(p-1)!\equiv -1 \pmod p$. This is *Wilson's theorem*.

Solution. The case $p=2$ is easy. For $p>2$, let x be a primitive root (mod p). Then

$$(p-1)!\equiv x^1x^2\cdots x^{p-1}=x^{(p-1)p/2} \pmod p.$$

By the property of x, $w=x^{(p-1)/2}$ satisfies $w\not\equiv 1 \pmod p$ and $w^2\equiv 1 \pmod p$. So $w\equiv -1 \pmod p$. Then

$$(p-1)!\equiv x^{(p-1)p/2}=w^p=-1 \pmod p.$$

Example 3. (1993 *Chinese IMO Team Selection Test*) For every prime number $p\geq 3$, define

$$F(p)=\sum_{k=1}^{(p-1)/2}k^{120},\quad f(p)=\frac{1}{2}-\left\{\frac{F(p)}{p}\right\},$$

where $\{x\}=x-[x]$ is the fractional part of x. Find the value of $f(p)$.

Solution. Let x be a primitive root (mod p). If $p-1\nmid 120$, then $x^{120}\not\equiv 1 \pmod p$ and $x^{120(p-1)}\equiv 1 \pmod p$. So

$$F(p)\equiv\frac{1}{2}\sum_{i=1}^{p-1}x^{120i}$$

$$=\frac{x^{120}(x^{120(p-1)}-1)}{2(x^{120}-1)}\equiv 0 \pmod p.$$

Then $f(p)=1/2$.

If $p-1\,|\,120$, then $p\in\{3, 5, 7, 11, 13, 31, 41, 61\}$ and $x^{120}\equiv 1 \pmod p$. So

$$F(p)\equiv\frac{1}{2}\sum_{i=1}^{p-1}x^{120i}=\frac{p-1}{2} \pmod p.$$

Then

$$f(p)=\frac{1}{2}-\frac{p-1}{2p}=\frac{1}{2p}.$$

Example 4. If a and b are nonnegative integers such that $2^a\equiv 2^b \pmod{101}$, then prove that $a\equiv b \pmod{100}$.

Solution. We first check 2 is a primitive root of (mod 101). If d is the least positive integer such that $2^d \equiv 1$ (mod 101), then dividing 100 by d, we get $100 = qd + r$ for some integers q, r, where $0 \le r < d$. By Fermat's little theorem,

$$1 \equiv 2^{100} = (2^d)^q 2^r \equiv 2^r \pmod{101},$$

which implies the remainder $r = 0$. So $d \mid 100$.

Assume $d < 100$. Then $d \mid 50$ or $d \mid 20$, which implies 2^{20} or $2^{50} \equiv 1$ (mod 101). But $2^{10} = 1024 \equiv 14 \pmod{101}$ implies $2^{20} \equiv 14^2 \equiv -6 \pmod{101}$ and $2^{50} \equiv 14(-6)^2 \equiv -1 \pmod{101}$. So $d = 100$.

Finally, $2^a \equiv 2^b \pmod{101}$ implies $2^{|a-b|} \equiv 1 \pmod{101}$. Then as above, dividing $|a-b|$ by 100, we will see the remainder is 0. Therefore, $a \equiv b \pmod{100}$.

Comments: The division argument in the solution above shows if $ord_n(x) = d$, then $x^k \equiv 1 \pmod{n}$ if and only if $d \mid k$. This is useful.

Example 5. (1994 *Putnam Exam*) For any integer a, set

$$n_a = 101a - 100 \times 2^a.$$

Show that for $0 \le a,b,c,d \le 99$,

$$n_a + n_b \equiv n_c + n_d \pmod{10100}$$

implies $\{a,b\} = \{c,d\}$.

Solution. Since 100 and 101 are relatively prime, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ is equivalent to

$$n_a + n_b \equiv n_c + n_d \pmod{100}$$

and

$$n_a + n_b \equiv n_c + n_d \pmod{101}.$$

As $n_a \equiv a \pmod{100}$ and $n_a \equiv 2^a \pmod{101}$. These can be simplified to

$$a + b \equiv c + d \pmod{100} \quad (*)$$

and

$$2^a + 2^b \equiv 2^c + 2^d \pmod{101}.$$

Using $2^{100} \equiv 1 \pmod{101}$ and (*), we get

$$2^a 2^b = 2^{a+b} \equiv 2^{c+d} = 2^c 2^d \pmod{101}.$$

Since $2^b \equiv 2^c + 2^d - 2^a \pmod{101}$, we get $2^a(2^c + 2^d - 2^a) \equiv 2^c 2^d \pmod{101}$. This can be rearranged as

$$(2^a - 2^c)(2^a - 2^d) \equiv 0 \pmod{101}.$$

Then $2^a \equiv 2^c \pmod{101}$ or $2^a \equiv 2^d \pmod{101}$. By the last example, we get $a \equiv c$ or $d \pmod{100}$. Finally, using $a + b \equiv c + d \pmod{100}$, we get $\{a,b\} = \{c,d\}$.

Example 6. Find all two digit numbers n (i.e. $n = 10a + b$, where $a, b \in \{0,1,\ldots,9\}$ and $a \ne 0$) such that for all integers k, we have $n \mid k^a - k^b$.

Solution. Clearly, $n = 11, 22, \ldots, 99$ work. Suppose n is such an integer with $a \ne b$. Let p be a prime divisor of n. Let x be a primitive root (mod p). Then $p \mid x^a - x^b$, which implies $x^{|a-b|} \equiv 1 \pmod{p}$. By the comment at the end of example 4, we have $p - 1 \mid |a-b| \le 9$. Hence, $p = 2$, 3, 5 or 7.

If $p = 7 \mid n$, then $6 \mid |a-b|$ implies $n = 28$. Now $k^2 \equiv k^8 \pmod 4$ and $\pmod 7$ hold by property of (mod 4) and Fermat's little theorem respectively. So $n = 28$ works.

Similarly the $p = 5$ case will lead to $n = 15$ or 40. Checking shows $n = 15$ works. The $p = 3$ case will lead to $n = 24$ or 48. Checking shows $n = 48$ works. The $p = 2$ case will lead to $n = 16$, 32 or 64, but checking shows none of them works. Therefore, the only answers are 11, 22, …, 99, 28, 15, 48.

Example 7. Let p be an odd prime number. Determine all functions $f: \mathbb{Z} \to \mathbb{Z}$ such that for all $m,n \in \mathbb{Z}$,

(i) if $m \equiv n \pmod{p}$, then $f(m) = f(n)$ and
(ii) $f(mn) = f(m)f(n)$.

Solution. For such functions, taking $m = n = 0$, we have $f(0) = f(0)^2$, so $f(0) = 0$ or 1. If $f(0) = 1$, then taking $m = 0$, we have $1 = f(0) = f(0) f(n) = f(n)$ for all $n \in \mathbb{Z}$, which is clearly a solution.

If $f(0) = 0$, then $n \equiv 0 \pmod{p}$ implies $f(n) = 0$. For $n \not\equiv 0 \pmod{p}$, let x be a primitive root (mod p). Then $n \equiv x^k \pmod{p}$ for some $k \in \{1,2,\ldots,p-1\}$. So $f(n) = f(x^k) = f(x)^k$. By Fermat's little theorem, $x^p \equiv x \pmod{p}$. This implies $f(x)^p = f(x)$. So $f(x) = 0$, 1 or -1. If $f(x) = 0$, then $f(n) = 0$ for all $n \in \mathbb{Z}$. If $f(x) = 1$, then $f(n) = 1$ for all $n \not\equiv 0 \pmod{p}$. If $f(x) = -1$, then for n congruent to a nonzero square number (mod p), $f(n) = 1$, otherwise $f(n) = -1$.

After seeing how primitive roots can solve problem, it is time to examine the proof of the theorem more closely. We will divide the proofs into a few observations.

For a polynomial $f(x)$ of degree n with coefficients in (mod p), the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions (mod p). This can be proved by doing induction on n and imitating the proof for real coefficient polynomials having at most n roots.

If $d \mid p-1$, then $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions (mod p). To see this, let $n = (p-1)/d$, then

$$x^{p-1} - 1 = (x^d - 1)(x^{(n-1)d} + x^{(n-2)d} + \cdots + 1).$$

Since $x^{p-1} - 1 \equiv 0 \pmod{p}$ has $p-1$ solutions by Fermat's little theorem, so if $x^d - 1 \equiv 0 \pmod{p}$ has less than d solutions, then

$$(x^d - 1)(x^{(n-1)d} + x^{(n-2)d} + \cdots + 1) \equiv 0 \pmod{p}$$

would have less than $d + (n-1)d = p-1$ solutions, which is a contradiction.

Suppose the prime factorization of $p-1$ is $p_1^{e_1} \cdots p_k^{e_k}$, where p_i's are distinct primes and $e_i \ge 1$. For $i = 1, 2, \ldots, k$, let $m_i = p_i^{e_i}$. Using the observation in the last paragraph, we see there exist $m_i - m_i/p_i > 1$ solutions x_i of equation $x^{m_i} - 1 \equiv 0 \pmod{p}$, which are not solutions of $x^{m_i/p_i} - 1 \equiv 0 \pmod{p}$. It follows that the least positive integer d such that $x_i^d - 1 \equiv 0 \pmod{p}$ is $m_i = p_i^{e_i}$. That means x_i has order $m_i = p_i^{e_i}$ in (mod p).

Let r be the order of $x_i x_j$ in (mod p). By the comment at the end of example 4, we have $r \mid p_i^{e_i} p_j^{e_j}$. Now

$$x_j^{rd} \equiv (x_i^d)^r x_j^{rd} = (x_i x_j)^{rd} \equiv 1 \pmod{p},$$

which by the comment again, we get $p_j^{e_j} \mid rd$. Since $p_j^{e_j}$ and $d = p_i^{e_i}$ are relatively prime, we get $p_j^{e_j} \mid r$. Interchanging the roles of p_i and p_j, we also get $p_j^{e_j} \mid r$. So $p_i^{e_i} p_j^{e_j} \mid r$. Then $r = p_i^{e_i} p_j^{e_j}$. So $x = x_1 x_2 \cdots x_k$ will have order $p_1^{e_1} \cdots p_k^{e_k} = p - 1$, which implies x is a primitive root (mod p).

For $n > 1$, Euler's theorem asserts that if x and n are relatively prime integers, then $x^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi(n)$ is the number of positive integers among $1,2,\ldots,n$ that are relatively prime to n. Similarly, we can define x to be a primitive root (mod n) if and only if the least positive integer d satisfying $x^d \equiv 1 \pmod{n}$ is $\varphi(n)$. For the inquisitive mind who wants to know for which n, there exists primitive roots (mod n), the answers are $n = 2$, 4, p^k and $2p^k$, where p is an odd prime. This is much harder to prove. The important thing is for such a primitive root x (mod n), the numbers $x^i \pmod{n}$ for $i = 1$ to $\varphi(n)$ is a permutation of the $\varphi(n)$ numbers among $1,2,\ldots,n$ that are relatively prime to n.

Problem Corner

We welcome readers to submit their solutions to the problems posed below for publication consideration. The solutions should be preceded by the solver's name, home (or email) address and school affiliation. Please send submissions to *Dr. Kin Y. Li, Department of Mathematics, The Hong Kong University of Science & Technology, Clear Water Bay, Kowloon, Hong Kong.* The deadline for sending solutions is ***July 10, 2010.***

Problem 346. Let k be a positive integer. Divide $3k$ pebbles into five piles (with possibly unequal number of pebbles). Operate on the five piles by selecting three of them and removing one pebble from each of the three piles. If it is possible to remove all pebbles after k operations, then we say it is a *harmonious ending*.

Determine a necessary and sufficient condition for a harmonious ending to exist in terms of the number k and the distribution of pebbles in the five piles.

(*Source*: 2008 *Zhejiang Province High School Math Competition*)

Problem 347. $P(x)$ is a polynomial of degree n such that for all $w \in \{1, 2, 2^2, \ldots, 2^n\}$, we have $P(w) = 1/w$.

Determine $P(0)$ with proof.

Problem 348. In ΔABC, we have $\angle BAC = 90^\circ$ and $AB < AC$. Let D be the foot of the perpendicular from A to side BC. Let I_1 and I_2 be the incenters of ΔABD and ΔACD respectively. The circumcircle of ΔAI_1I_2 (with center O) intersects sides AB and AC at E and F respectively. Let M be the intersection of lines EF and BC.

Prove that I_1 or I_2 is the incenter of the ΔODM, while the other one is an excenter of ΔODM.

(*Source:* 2008 *Jiangxi Province Math Competition*)

Problem 349. Let $a_1, a_2, \ldots, a_n$ be rational numbers such that for every positive integer m,

$$a_1^m + a_2^m + \cdots + a_n^m$$

is an integer. Prove that $a_1, a_2, \ldots, a_n$ are integers.

Problem 350. Prove that there exists a positive constant c such that for all positive integer n and all real numbers $a_1, a_2, \ldots, a_n$, if

$$P(x) = (x - a_1)(x - a_2) \cdots (x - a_n),$$

then

$$\max_{x\in[0,2]} |P(x)| \le c^n \max_{x\in[0,1]} |P(x)|.$$

****

Solutions

****

Problem 341. Show that there exists an infinite set S of points in the 3-dimensional space such that every plane contains at least one, but not infinitely many points of S.

Solution. **Emanuele NATALE and Carlo PAGANO** (Università di Roma "Tor Vergata", Roma, Italy).

Consider the curve $\sigma : \mathbb{R} \to \mathbb{R}^3$ defined by $\sigma(x) = (x, x^3, x^5)$. Let S be the graph of σ. If $ax+by+cz=d$ is the equation of a plane in $\mathbb{R}^3$, then the intersection of the plane and the curve is determined by the equation

$$ax + bx^3 + cx^5 = d,$$

which has at least one and at most five solutions.

Other commended solvers: **HUNG Ka Kin Kenneth** (Diocesan Boys' School), **D. Kipp JOHNSON** (Valley Catholic School, Beaverton, Oregon, USA) and **LI Pak Hin** (PLK Vicwood K. T. Chong Sixth Form College).

Problem 342. Let $f(x)=a_nx^n+\cdots+a_1x+p$ be a polynomial with coefficients in the integers and degree $n>1$, where p is a prime number and

$$|a_n|+|a_{n-1}|+\cdots+|a_1| < p.$$

Then prove that $f(x)$ is not the product of two polynomials with coefficients in the integers and degrees less than n.

Solution. **The 6B Mathematics Group** (Carmel Alison Lam Foundation Secondary School)**, CHUNG Ping Ngai** (La Salle College, Form 6), **LEE Kai Seng** (HKUST), **LI Pak Hin** (PLK Vicwood K. T. Chong Sixth Form College), **Emanuele NATALE** (Università di Roma "Tor Vergata", Roma, Italy), **Pedro Henrique O. PANTOJA** (University of Lisbon, Portugal).

Let w be a root of $f(x)$ in $\mathbb{C}$. Assume $|w| \le 1$. Using $a_nw^n+\cdots+a_1w+p=0$ and the triangle inequality, we have

$$p = \left|\sum_{i=1}^{n} a_i w^i\right| \le \sum_{i=1}^{n} |a_i|\,|w|^i \le \sum_{i=1}^{n} |a_i|,$$

which contradicts the given inequality. So all roots of $f(x)$ have absolute values greater than 1.

Assume $f(x)$ is the product of two integral coefficient polynomials $g(x)$ and $h(x)$ with degrees less than n. Let b and c be the nonzero coefficients of the highest degree terms of $g(x)$ and $h(x)$ respectively. Then $|b|$ and $|c| \ge 1$. By Vieta's theorem, $|g(0)/b|$ and $|h(0)/c|$ are the products of the absolute values of their roots respectively. Since their roots are also roots of $f(x)$, we have $|g(0)/b| > 1$ and $|h(0)/c| > 1$. Now $p = |f(0)| = |g(0)h(0)|$, but $g(0)$, $h(0)$ are integers and $|g(0)| > |b| \ge 1$ and $|h(0)| > |c| \ge 1$, which contradicts p is prime.

Problem 343. Determine all ordered pairs (a,b) of positive integers such that $a \ne b$, $b^2+a=p^m$ (where p is a prime number, m is a positive integer) and a^2+b is divisible by b^2+a.

Solution. **CHUNG Ping Ngai** (La Salle College, Form 6), **HUNG Ka Kin Kenneth** (Diocesan Boys' School) and **LI Pak Hin** (PLK Vicwood K. T. Chong Sixth Form College).

For such (a,b),

$$\frac{a^2+b}{a+b^2} = a - b^2 + \frac{b^4+b}{a+b^2}$$

implies $p^m = a + b^2 \mid b^4 + b = b(b^3+1)$. From $a \ne b$, we get $b < 1+b < a+b^2$. As $\gcd(b, b^3+1) = 1$, so p^m divides $b^3+1 = (b+1)(b^2-b+1)$.

Next, by the Euclidean algorithm, we have $\gcd(b+1,b^2-b+1) = \gcd(b+1,3) \mid 3$.

Assume we have $\gcd(b+1,b^2-b+1)=1$. Then $b^2+a=p^m$ divides only one of $b+1$ or b^2-b+1. However, both $b+1$, $b^2-b+1 < b^2+a=p^m$. Hence, $b+1$ and b^2-b+1 must be divisible by p. Then the assumption is false and

$$p = \gcd(b+1,b^2-b+1) = 3. \qquad (*)$$

If $m = 1$, then $b^2+a = 3$ has no solution. If $m = 2$, then $b^2+a = 9$ yields $(a,b) = (5,2)$.

For $m \ge 3$, by (*), one of $b+1$ or b^2-b+1 is divisible by 3, while the other one is divisible by 3^{m-1}. Since

$$b + 1 < \sqrt{b^2+a} + 1 = 3^{m/2} + 1 < 3^{m-1},$$

so $3^{m-1} \mid b^2-b+1$. Since $m \ge 3$, we have $b^2 - b + 1 \equiv 0 \pmod 9$. Checking $b \equiv -4, -3, -2, -1, 0, 1, 2, 3, 4 \pmod 9$ shows there cannot be any solution.

Problem 344. *ABCD* is a cyclic quadrilateral. Let *M, N* be midpoints of diagonals *AC, BD* respectively. Lines *BA, CD* intersect at *E* and lines *AD, BC* intersect at *F*. Prove that

$$\left|\frac{BD}{AC}-\frac{AC}{BD}\right|=\frac{2MN}{EF}.$$

***Solution* 1. LEE Kai Seng** (HKUST)**.**

Without loss of generality, let the circumcircle of *ABCD* be the unit circle in the complex plane. We have

$$M=(A+C)/2 \quad \text{and} \quad N=(B+D)/2.$$

The equations of lines *AB* and *CD* are

$$Z+AB\overline{Z}=A+B$$

and

$$Z+CD\overline{Z}=C+D$$

respectively. Solving for *Z*, we get

$$E=Z=\frac{\overline{A}+\overline{B}-\overline{C}-\overline{D}}{\overline{AB}-\overline{CD}}.$$

Similarly,

$$F=\frac{\overline{A}-\overline{B}-\overline{C}+\overline{D}}{\overline{AD}-\overline{BC}}.$$

In terms of *A, B, C, D*, we have

$$2MN=|A+C-B-D|,$$

$$\begin{aligned}EF&=\left|\overline{E}-\overline{F}\right|\\&=\left|\frac{A+B-C-D}{AB-CD}-\frac{A-B-C+D}{AD-BC}\right|\\&=\left|\frac{(B-D)(C-A)(A+C-B-D)}{(AB-CD)(AD-BC)}\right|.\end{aligned}$$

The left and right hand sides of the equation become

$$\left|\frac{BD}{AC}-\frac{AC}{BD}\right|=\left|\frac{|B-D|^2-|A-C|^2}{(A-C)(B-D)}\right|,$$

$$\frac{2MN}{EF}=\left|\frac{(AB-CD)(AD-BC)}{(B-D)(C-A)}\right|.$$

It suffices to show the numerators of the right sides are equal. We have

$$\begin{aligned}&\left||B-D|^2-|A-C|^2\right|\\&=\left|(B-D)(\overline{B}-\overline{D})-(A-C)(\overline{A}-\overline{C})\right|\\&=\left|A\overline{C}+C\overline{A}-B\overline{D}-D\overline{B}\right|\end{aligned}$$

and

$$\begin{aligned}&\left|(AB-CD)(AD-BC)\right|\\&=\left|(AB-CD)(\overline{AD}-\overline{BC})\right|\\&=\left|B\overline{D}-C\overline{A}-A\overline{C}+D\overline{B}\right|.\end{aligned}$$

Comments: For complex method of solving geometry problems, please see Math Excalibur, *vol*. 9, *no*. 1.

***Solution* 2. CHUNG Ping Ngai** (La Salle College, Form 6).

Without loss of generality, let $AC > BD$. Since $\angle EAC=\angle EDB$ and $\angle AEC=\angle DEB$, we get $\Delta AEC\sim\Delta DEB$. Then

$$\frac{AE}{DE}=\frac{AC}{DB}=\frac{AM}{DN}=\frac{MC}{DB}$$

and $\angle ECA=\angle EBD$. So $\Delta AEM\sim\Delta DEN$ and $\Delta CEM\sim\Delta BEN$. Similarly, we have $\Delta AFC\sim\Delta BFD$, $\Delta AFM\sim\Delta BFN$ and $\Delta CFM\sim\Delta DFN$. Then

$$\frac{EN}{EM}=\frac{DE}{AE}=\frac{BD}{AC}=\frac{FB}{FA}=\frac{FN}{FM}. \quad (*)$$

Define *Q* so that *QENF* is a parallelogram. Let $P=MQ\cap EF$. Then

$$\begin{aligned}\angle EQF&=\angle FNE=180^\circ-\angle ENB-\angle FND\\&=180^\circ-\angle EMC-\angle FMC=180^\circ-\angle EMF.\end{aligned}$$

Hence, *M, E, Q, F* are concyclic. Then $\angle MEQ=180^\circ-\angle MFQ$.

By (1), $EN\times FM=EM\times FN$. Then

$$\begin{aligned}[EMQ]&=\tfrac{1}{2}EM\times FN\sin\angle MEQ\\&=\tfrac{1}{2}EN\times FM\sin\angle MFQ=[FMQ],\end{aligned}$$

where $[XYZ]$ denotes the area of ΔXYZ. Then *EP=FP*, which implies *M, N, P, Q* are collinear. Due to *M, E, Q, F* concyclic, so $\Delta PEM\sim\Delta PQF$ and $\Delta PEQ\sim\Delta PMF$. Then

$$\frac{EM}{EN}=\frac{EM}{QF}=\frac{PM}{PF},\quad \frac{FN}{FM}=\frac{QE}{FM}=\frac{QP}{PF}=\frac{NP}{PF}.$$

Using these relations, we have

$$\begin{aligned}\frac{AC}{BD}-\frac{BD}{AC}&=\frac{EM}{EN}-\frac{FN}{FM}\\&=\frac{MP}{PF}-\frac{NP}{PF}=\frac{MN}{EF/2},\end{aligned}$$

which is the desired equation.

Problem 345. Let $a_1, a_2, a_3, \cdots$ be a sequence of integers such that there are infinitely many positive terms and also infinitely many negative terms. For every positive integer *n*, the remainders of $a_1, a_2, \cdots, a_n$ upon divisions by *n* are all distinct. Prove that every integer appears exactly one time in the sequence.

Solution. **CHUNG Ping Ngai** (La Salle College, Form 6), **HUNG Ka Kin Kenneth** (Diocesan Boys' School), **LI Pak Hin** (PLK Vicwood K. T. Chong Sixth Form College), **Emanuele NATALE and Carlo PAGANO** (Università di Roma "Tor Vergata", Roma, Italy).

Assume there are $i > j$ such that $a_i = a_j$. Then for $n > i$, $a_i \equiv a_j \pmod n$, which is a contradiction. So any number appears at most once.

Next, for every positive integer *n*, let $S_n=\{a_1, a_2, \ldots, a_n\}$, $\max S_n = a_v$ and $\min S_n = a_w$. If $k = a_v - a_w \ge n$, then $k \ge n \ge v, w$ and $a_v \equiv a_w \pmod k$, contradicting the given fact. So

$$\max S_n - \min S_n = a_v - a_w \le n-1.$$

Now $S_n \subseteq [\min S_n, \max S_n]$ and both contain *n* integers. So the *n* numbers in S_n are the *n* consecutive integers from $\min S_n$ to $\max S_n$.

Now for every integer *m*, since there are infinitely many positive terms and also infinitely many negative terms, there exists a_p and a_q such that $a_p < m < a_q$. Let $r > \max\{p,q\}$, then *m* is in S_r. Therefore, every integer appears exactly one time in the sequence.

Comment: An example of such a sequence is 0, 1, −1, 2, −2, 3, −3, ….

Olympiad Corner

(continued from page 1)

Problem 4. Let $a \in \mathbb{N}$ be such that for every $n \in \mathbb{N}$, $4(a^n+1)$ is a perfect cube. Show that $a = 1$.

Problem 5. We want to choose some phone numbers for a new city. The phone numbers should consist of exactly ten digits, and 0 is not allowed as a digit in them. To make sure that different phone numbers are not confused with each other, we want every two phone numbers to either be different in at least two places or have digits separated by at least 2 units, in at least one of the ten places.

What is the maximum number of phone numbers that can be chosen, satisfying the constraints? In how many ways can one choose this amount of phone numbers?

Problem 6. Let *ABC* be a triangle and *H* be the foot of the altitude drawn from *A*. Let *T, T'* be the feet of the perpendicular lines drawn from *H* onto *AB, AC*, respectively. Let *O* be the circumcenter of ΔABC, and assume that $AC = 2OT$. Prove that $AB = 2OT'$.