Mathematical Excalibur

Volume 17, Number 3 *November-December 2012*

Olympiad Corner

Below are the problems of the 15th Hong Kong China Math Olympiad.

Problem 1. For any positive integer n, let a_1, a_2, …, a_m be all the positive divisors of n, where $m\geq 1$. If there exist m integers b_1, b_2, …, b_m such that

$$n=\sum_{i=1}^{m}(-1)^{b_i}a_i,$$

then we say that n is a *good number*. Prove that there exists a good number with exactly 2013 distinct prime factors.

Problem 2. Some of the lattice points (x,y), with $1\leq x\leq 101$ and $1\leq y\leq 101$ are marked so that no 4 marked points form the vertices of an isosceles trapezoid with bases parallel to the x-axis or the y-axis (a rectangle is counted as an isosceles trapezoid). Determine the maximum number of marked points. (A lattice point is a point with integral coordinates.)

Problem 3. Prove that for every positive integer n and every group of real numbers a_1, a_2, …, $a_n > 0$,

$$\sum_{k=1}^{n}\frac{k}{a_1^{-1}+a_2^{-1}+...+a_k^{-1}}\leq 2\sum_{k=1}^{n}a_k.$$

(continued on page 4)

Editors: 張 百 康 (CHEUNG Pak-Hong), Munsang College, HK
高 子 眉 (KO Tsz-Mei)
梁 達 榮 (LEUNG Tat-Wing)
李 健 賢 (LI Kin-Yin), Dept. of Math., HKUST
吳 鏡 波 (NG Keng-Po Roger), ITC, HKPU

Artist: 楊 秀 英 (YEUNG Sau-Ying Camille), MFA, CU

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 ***February 3, 2013***.

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

Primes in Arithmetic Progressions

Kin Y. Li

To see there are infinitely many prime numbers, we assume only finitely many of them exist, say $p_1,p_2,\ldots,p_m$. Consider $q = p_1p_2\cdots p_m+1$. Let p be a prime in the prime factorization of q. Then p is one of the p_i's. So p divides q and $q-1$. Then p divides $q-(q-1)=1$, contradiction.

Other than 2, the rest of the prime numbers are in the arithmetic progression $2n+1$, where n denotes a positive integer. It is natural to ask how many prime numbers are in the other arithmetic progressions $an+b$, where a and b are given integers with $a>0$. Certainly, if gcd$(a,b)>1$, then no primes will be in the sequence $an+b$.

In case $(a,b)=(4,-1)$ we can see the answer is infinitely many by modifying the proof above. Assume $p_1,p_2,\ldots,p_m$ are all the primes of the form $4n-1$. Then let $q=4p_1p_2\cdots p_m-1$. Now $q\equiv -1$ (mod 4). Assume q is a product of primes in the sequence $4n+1$. Then $q\equiv 1$ (mod 4), contradiction. So q must have at least one prime divisor p in the sequence $4n-1$. Then p is one of the p_i's. So p divides q and $q+1$. Then p divides $(q+1)-q=1$, contradiction.

In case $(a,b)=(p,1)$, where p is a prime, we will need facts from number theory.

Fact 1 (Bezout's Theorem). For all positive integers a and b, there exist integers r and s such that $ar+bs$ = gcd(a,b).

Fact 2 (Euler's Theorem). For positive integer n, let $\varphi(n)$ be the number of integers among $1,2,\ldots,n$ that is relatively prime to n. If gcd$(a,n)=1$, then $a^{\varphi(n)}\equiv 1$ (mod n). In case n is a prime, we have $\varphi(n)=n-1$ and $a^{n-1}\equiv 1$ (mod n). This case is *Fermat's Little Theorem*.

Example 1 (*2004 Korean Mathematical Olympiad*). Let p be a prime and $f_p(x) = x^{p-1}+x^{p-2}+\cdots+x+1$.

(1) For each integer m divisible by p, is there an integer q such that q divides $f_p(m)$ and gcd$(q,m(m-1))=1$?

(2) Prove that there are infinitely many integers n such that $pn+1$ is prime.

Solution. (1) Yes. Let q be a prime divisor of $f_p(m)$. As $f_p(m)\equiv 1$ (mod m), we see q does not divide m. Hence gcd$(m,q)=1$. Assume $m\equiv 1$ (mod q). Then $0\equiv f_p(m)\equiv p$ (mod q), which implies $p=q$. Since p divides m, we get $1\equiv f_p(m)\equiv p$ (mod p), contradiction. Hence q does not divide $m-1$. Then gcd$(q,m(m-1))=1$.

(2) Assume $p_1,p_2,\ldots,p_k$ are all the primes of the form $pn+1$. Let $m = p_1p_2\cdots p_k\,p$ and q be a prime divisor of $f_p(m)$. By (1), $m\not\equiv 0$ or 1 (mod q), which implies gcd$(m,q)=1$. By Fermat's little theorem, $m^{q-1}\equiv 1$ (mod q). Now $m^p-1 = (m-1)\,f_p(m)$ implies $m^p\equiv 1$ (mod q).

Assume gcd$(q-1,p)=1$. By Bezout's theorem, there are integers r and s such that $(q-1)r+ps=1$. Then $m=m^{(q-1)r}m^{ps}$ $\equiv$ 1 (mod q), contradicting the last underlined expression. Then gcd$(q-1,p)$ = p, i.e. q is of the form $pn+1$. As q divides $f_p(m)$ and $f_p(m)\equiv 1$ (mod p_i), we see $q\neq p_1,p_2,\ldots,p_k$.

In the general case gcd$(a,b)>1$, we have

Dirichlet's Theorem. If a and b are given integers with $a>0$ and gcd$(a,b)>1$, then there are infinitely many primes in the arithmetic progression $an+b$.

All known proof of this theorem is beyond the scope of secondary school curriculum. Below we will look at some examples. First we need more facts.

Fact 3 (Chinese Remainder Theorem). If k_1, k_2, …, k_n are pairwise relatively prime positive integers and c_1, c_2, …, c_n are integers, then there exist a unique integer x in the interval $[1, k_1k_2\cdots k_n]$ such that $x\equiv c_i$ (mod k_i) for $i=1,2,\ldots, n$.

Fact 4 (Wilson's Theorem). If p is a prime, then $(p-1)!\equiv -1$ (mod p).

At the end of the article, we will give explanations for facts 1 to 4.

Example 2 (*1996 St Petersburg Math Olympiad*) Prove that there are no positive integers a and b such that for each pair p, q of distinct primes greater than 1000, the number $ap+bq$ is also prime.

Solution. Assume such a and b exist. Let r be a prime number with $\gcd(r,a)=\gcd(r,b)=1$. By Dirichlet's theorem, there exist positive integers x and y such that $p=rx+b$ and $q=ry-a$ are prime numbers greater than 1000. Then $ap+bq=(ax+by)r$ is not prime, contradiction.

Example 3 (*1997 British Mathematical Olympiad*) Let $S = \{1/r : r = 1,2,3,\ldots\}$. For all integer $k > 1$, prove that there is a k-term arithmetic progression in S such that no addition term in S can be added to it to form a $(k+1)$-term arithmetic progression.

Solution. By Dirichlet's theorem, there exists a positive integer n such that $kn+1$ is prime. Let $a_1=1/(kn)!$ and $d=n/(kn)!$. For $i=2,\ldots,k$, $a_i=a_1+(i-1)d$ $=(1+(i-1)n)/(kn)!$ are in S. However, the term $a_{k+1}=a_1+kd=(kn+1)/(kn)!$ is not in S since $kn+1$ is a prime. So a_1, a_2, …, a_k is such an example.

Example 4 Prove that for every positive integer s, a, b with $\gcd(a,b)=1$, there are infinitely many integers n such that $an+b$ is a product of s pairwise distinct prime numbers.

Solution. The case s=1 is Dirichlet's theorem. Suppose the case s is true. Then there exists an integer N such that $aN+b= q_1q_2\cdots q_s$, where q_1, q_2, …, q_s. are pairwise distinct primes. Next, by Dirichlet's theorem, there exist infinitely many positive integers n such that $an+1$ is a prime greater than all of q_1, q_2, …, q_s. Let $t_n= q_1q_2\cdots q_sn+N$. Then $at_n+b = aq_1q_2\cdots q_sn+aN+$b $= q_1q_2\cdots q_s(an+1)$ is a product of $s+1$ pairwise distinct prime numbers. This completes the induction.

Example 5 (*2011 Mongolian Math Olympiad Team Selection Test*) Let m be a positive odd integer. Prove that there exist infinitely many positive integer n such that $(2^n-1)/(mn+1)$ is an integer.

Solution. By Dirichlet's theorem, there exist infinitely many primes $p > m$ and $p= \varphi(m)k+1$ for some positive integer k. By Euler's theorem, $2^{\varphi(m)} \equiv 1$ (mod m). Then

$$2^p = 2^{\varphi(m)k+1} \equiv 2 \pmod{m}.$$

This leads to $n=(2^p-2)/m$ is an integer. By Fermat's little theorem, p divides $2^p - 2$. Since $p>m$, we see p divides n. Then $mn+1=2^p-1$ divides 2^n-1. Therefore, $(2^n-1)/(mn+1)$ is an integer.

Example 6 (*American Math Monthly 4772*) Let p_k be the k-th prime number. For every integer N, prove that there exists a positive integer k such that both p_{k-1} and p_{k+1} are not in the interval $[p_k-N, p_k+N]$.

Solution. Let q be a prime number greater than N+2. Observe that $a=q!$ and $b=(q-1)!-1$ are relatively prime because the prime divisors of $q!$ are the primes less than or equal to q, however $(q-1)!-1$ is not divisible by any prime number less than q and $(q-1)!-1 \equiv -2$ (mod q) by Wilson's theorem.

By Dirichlet's theorem, there is a prime $p_k \equiv (q-1)!-1$ (mod $q!$). Then $p_k+1\equiv 0$ (mod $(q-1)!$). Also, by Wilson's theorem, $p_k+2 \equiv (q-1)!+1\equiv 0$ (mod q). These showed p_k+1 and p_k+2 are not primes. For $j=2,\ldots, q-1$, we have

$$p_k+1\pm j \equiv p_k+1 \equiv (q-1)! \equiv 0 \pmod{j}.$$

So integers in $[p_k-q+2, p_k+q]$ except p_k are not primes. Since $q>N+2$, both p_{k-1} and p_{k+1} cannot be in the $[p_k-N, p_k+N]$.

Example 7 (*American Math Monthly E1632*) Prove that if $f(x)$ is a polynomial with rational coefficients such that $f(p)$ is a prime number for every prime number p, then either $f(x)=x$ for all x or $f(x)$ is the same prime constant for all x.

Solution. Assume the conclusion is false. Let k be the least common multiple of the denominators of the coefficients of $f(x)$ and let $g(x)=kf(x)$. Then $g(x)$ has integer coefficients. Now there must be a prime p such that p and $g(p)$ are relatively prime (otherwise, for the infinitely many primes p that are relatively prime to k, we have $\gcd(p,g(p))=p$, so p divides $g(p)=kf(p)$, hence both primes $f(p)$ and p are equal, which forces $f(x)=x$).

By Dirichlet's theorem, there are infinitely many integers n_i such that $m_i=g(p)n_i+p$ is prime. Now $g(m_i) \equiv g(p) \equiv 0$ (mod $g(p)$) for all i. Then $kf(p)$ divides $kf(m_i)$. Hence $f(p)$ divides $f(m_i)$. Since $f(p)$ and $f(m_i)$ are primes, we get $f(m_i)=f(p)$ for infinitely many i. This leads to $f(x)$ being the constant polynomial $f(p)$, contradiction.

Example 8 (*American Math Monthly 4524*) Prove that for every pair of positive integers n and N, there are consecutive positive integers k, k+1, …, $k+N$ such that $\varphi(k)$, $\varphi(k+1)$, …, $\varphi(k+N)$ are all divisible by n, where $\varphi(n)$ is as defined in Euler's theorem.

Solution. We need the *fact* that if integer $w=ab$, where $a=p^m$, p is prime and $\gcd(b,p)=1$, then $\varphi(w)$ is divisible by $p-1$.

Granting the *fact*, by Dirichlet's theorem, there are distinct primes p_0, p_1, …, $p_N \equiv 1$ (mod n). By the Chinese remainder theorem, there is an integer k such that $k \equiv 0$ (mod p_0), $k \equiv -1$ (mod p_1),…, $k\equiv -N$ (mod p_N). So for j=0,1, …, N, the number $k+j$ is divisible by the prime p_j. Then $\varphi(k+j)$ is divisible by p_j-1 by the fact, which is a multiple of n.

For the *fact*, note $\gcd(a,b)=1$. Then $\varphi(ab)= \varphi(a)\varphi(b)$. (This follows from the Chinese remainder theorem, since for every k in $[1,ab]$ with $\gcd(k,ab)=1$, let r and s be the remainders when k is divided by a and b respectively. Now $\gcd(k,ab)=1$ if and only if $\gcd(r,a) = 1 = \gcd(s,b)$. The Chinese remainder theorem asserts that $x \equiv k$ (mod ab) if and only if $x \equiv r$ (mod a) and $x \equiv s$ (mod b). Thus $x\leftrightarrow(r,s)$ is bijective.) For x in $[1,p^m]$, $\gcd(x,p^m)>1$ if and only if x is a multiple of p. So $\varphi(a)=\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$. Then $\varphi(w)= \varphi(a)\varphi(b)$ is divisible by $p-1$.

Example 9 Prove that there are infinitely many positive integers n such that the equation $x^n+y^n=z^n$ has no solution (x,y,z) in integers with $xyz\neq 0$ and $\gcd(n,xyz)=1$. (*These n's may even be chosen to be pairwise relatively prime.*)

(*Remark* Barry Powell published this result in the *American Mathematical Monthly* on November 1978.)

Solution. The case n=4 is well-known. Next, suppose n_1, n_2, …, n_k are such n's. By Dirichlet's theorem, there is a prime p such that $p \equiv -1$ (mod $4n_1n_2\cdots n_k$). We define a new $n = p(p-1)/2$. Note $n \equiv 1$ (mod 4). Since $(p-1)/2$, $(p+1)/2$ are consecutive integers and $p > (p+1)/2$, so $\gcd(p(p-1)/2, (p+1)/2) = 1$. Hence, $\gcd(n, 4n_1n_2\cdots n_k)=1$. (*In particular, n is relatively prime to every one of n_1, n_2, ..., n_k.*)

(continued on page 4)

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 ***February 3, 2013.***

Problem 406. For every integer $m>2$, let P be the product of all those positive integers that are less than m and relatively prime to m, prove that P^2-1 is divisible by m.

Problem 407. Three circles S, S_1, S_2 are given in a plane. S_1 and S_2 touch each other externally, and both of them touch S internally at A_1 and at A_2 respectively. Let P be one of the two points where the common internal tangent to S_1 and S_2 meets S. Let B_i be the intersection points of PA_i and S_i (i=1,2). Prove that line B_1B_2 is a common tangent to S_1 and S_2.

Problem 408. Let $\mathbb{Q}$ denote the set of all rational numbers. Let f:$\mathbb{Q}\rightarrow\{0,1\}$ be a function such that for all x,y in $\mathbb{Q}$ with $f(x)=f(y)$, we have $f((x+y)/2)=f(x)$. If $f(0)=0$ and $f(1)=1$, then prove that $f(x)=1$ for every rational $x>1$.

Problem 409. The population of a city is one million. Every two citizens there know another common citizen (here knowing is mutual). Prove that it is possible to choose 5000 citizens from the city such that each of the remaining citizens will know at least one of the chosen citizens.

Problem 410. (*Due to Titu ZVONARU and Neculai STANCIU, Romania*) Prove that for all positive real x,y,z,

$$\sum_{cyc}(x+y)\sqrt{(x+z)(y+z)}\geq 4(xy+yz+zx)$$

$$+\frac{xy+yz+zx}{3(x^2+y^2+z^2)}((x-y)^2+(y-z)^2+(z-x)^2).$$

Here $\sum_{cyc}f(x,y,z)=f(x,y,z)+f(y,z,x)+f(z,x,y)$.

****

Solutions

****

Problem 401. Suppose all faces of a convex polyhedron are parallelograms. Can it have exactly 2012 faces? Please provide an explanation to your answer.

Solution. **CHEUNG Ka Wai** (Munsang College (Hong Kong Island)) and **F5 Group** (Carmel Alison Lam Foundation Secondary School).

The answer is negative. Let us call a series of faces $F_1, F_2,\ldots, F_k$ a <u>*loop*</u> if the pairs $(F_1, F_2), (F_2, F_3),\ldots, (F_{k-1}, F_k), (F_k, F_1)$ each have a common edge and all these common edges are parallel. Clearly any two loops have exactly two common faces and conversely each face belongs to exactly two loops. Therefore, if there are n loops, the total number of faces must be $2\ {}_nC_2=n(n-1)$. However, $n(n-1)=2002$ has no solution in integer.

Problem 402. Let S be a 30 element subset of $\{1,2,\ldots,2012\}$ such that every pair of elements in S are relatively prime. Prove that at least half of the elements of S are prime numbers.

Solution. **CHEUNG Ka Wai** (Munsang College (Hong Kong Island)), **F5 Group** (Carmel Alison Lam Foundation Secondary School), **KWAN Chung Hang** (Sir Ellis Kadoorie Secondary School (West Kowloon)), **Cyril LETROUIT** (Lycée Jean-Baptiste Say, Paris, France), **ZOLBAYAR Shagdar** (Orchlon International School, Ulaanbaatar, Mongolia) and **Titu ZVONARU** (Comăneşti, Romania) and **Neculai STANCIU** ("George Emil Palade" Secondary School, Buzău, Romania).

Assume there are more than 15 elements in S are not prime. Excluding 1, there are at least 15 of them are composite numbers. Each composite number in S has a prime divisor at most $[2012^{1/2}] = 46$. There are 14 prime numbers less than 46. By the pigeonhole principle, two of the 15 composite numbers above will share a common prime divisor, contradiction.

Problem 403. On the coordinate plane, 1000 points are randomly chosen. Prove that there exists a way of coloring each of the points either red or blue (but not both) so that on every line parallel to the x-axis or y-axis, the number of red points minus the number of blue points is equal to −1, 0 or 1.

Solution. **J. S. GLIMMS** (Vancouver, Canada) and **Cyril LETROUIT** (Lycée Jean-Baptiste Say, Paris, France).

Replace 1000 by n. We prove by induction on n. The case n=1 is clear. Suppose the case n=k is true. For the case n=k+1, we have two cases.

<u>*Case A*</u> (one of the lines L parallel to the x-axis or the y-axis contains an odd number of the points). Ignore one of the points P on L. By inductive step, there is a desired coloring for the remaining k points. Since there is an even number of point on L now, the number of red and blue points must be the same. Then look at the coloring on the line $L^\perp$ through P perpendicular to L. Color P red if $L^\perp$ is a −1 or 0 case and blue if it is a 1 case.

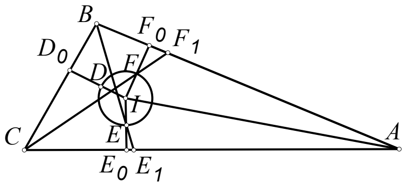
<u>*Case B*</u> (all lines parallel to the x-axis or y-axis contain an even number of the points). Ignore one of the points P on one of the lines L parallel to the x-axis. By inductive step, there is a desired coloring for the remaining k points. Let $L^\perp$ be the line through P parallel to the y-axis.

Since other than L, the lines parallel to x-axis all contain an even number of the points, they must all be 0 case lines. Ignoring P, if L is a case 1 line, then in the whole plane there is exactly one more red point than blue point. Also, other than $L^\perp$, the lines parallel to y-axis all contain an even number of the points, they must all be 0 case lines. Then $L^\perp$ must also be a case 1 line. We then color P blue so both L and $L^\perp$ become case 0 lines. Similarly, ignoring P, both lines may be 0 cases, then color P red or blue. Otherwise both lines are −1 cases, then color P red.

Other commended solvers: **F5 Group** (Carmel Alison Lam Foundation Secondary School).

Problem 404. Let I be the incenter of acute ΔABC. Let Γ be a circle with center I that lies inside ΔABC. D, E, F are the intersection points of circle Γ with the perpendicular rays from I to sides BC, CA, AB respectively. Prove that lines AD, BE, CF are concurrent.

Solution. **F5 Group** (Carmel Alison Lam Foundation Secondary School) and **J. S. GLIMMS** (Vancouver, Canada).



(Below P=α∩β will mean lines α and β meet at point P, $d(P$,α) will denote the distance from point P to line α and $[XYZ]$ will denote the area of ΔXYZ.)

Let $D_0 = ID\cap BC$, $E_0 = IE\cap CA$, $F_0 = IF\cap AB$. Since AI bisects $\angle CAB$, IE_0 and IF_0 are symmetric respect to AI. Now $IE=IF$ implies E and F are symmetric respect to AI. Hence, $d(E,AB)=d(F,AC)$. Then

$$\frac{[CFA]}{[AEB]}=\frac{CA\cdot d(F,AC)/2}{AB\cdot d(E,AB)/2}=\frac{CA}{AB}.$$

Similarly,

$$\frac{[BEC]}{[CDA]}=\frac{BC}{CA}\quad and\quad \frac{[ADB]}{[BFC]}=\frac{AB}{BC}.$$

Let $D_1 = AD\cap BC$, $E_1 = BE\cap CA$, $F_1 = CF\cap AB$. We have

$$\frac{AF_1}{F_1B}=\frac{[CF_1A]}{[BF_1C]}=\frac{d(A,CF)}{d(B,CF)}=\frac{[CFA]}{[BFC]}.$$

Similarly,

$$\frac{BD_1}{D_1C}=\frac{[ADB]}{[CDA]}\quad and\quad \frac{CE_1}{E_1A}=\frac{[BEC]}{[AEB]}.$$

From the equations above, we get

$$\frac{AF_1}{F_1B}\frac{BD_1}{D_1C}\frac{CE_1}{E_1A}=\frac{CA}{BC}\frac{AB}{CA}\frac{BC}{AB}=1.$$

By Ceva's theorem, lines AD, BE, CF are concurrent.

Other commended solvers: **MANOLOUDIS Apostolos** (4° Lyk. Korydallos, Piraeus, Greece).

Comment: **Titu ZVONARU** (Comăneşti, Romania) and **Neculai STANCIU** ("George Emil Palade" Secondary School, Buzău, Romania) mentioned that the problem was well-known and the point of concurrency is called the Kariya point.

Problem 405. Determine all functions f,g: $(0,+\infty) \to (0,+\infty)$ such that for all positive number x, we have

$$f(g(x))=\frac{x}{xf(x)-2}\quad and\quad g(f(x))=\frac{x}{xg(x)-2}.$$

Solution. **F5 Group** (Carmel Alison Lam Foundation Secondary School) and **J. S. GLIMMS** (Vancouver, Canada).

Let $F(x)=xf(x)$ and $G(x)=xg(x)$. For all $x > 0$, $f(g(x)) > 0$ and $g(f(x)) > 0$ imply $F(x)>2$ and $G(x)>2$. Define $a_1=2$. Now

$$\frac{G(x)}{F(x)-2}=g(x)f(g(x))=F(g(x))>a_1.$$

Then $\quad G(x) > a_1F(x) -2a_1. \qquad (1)$

Similarly, $\quad F(x) > a_1G(x) -2a_1. \qquad (2)$

Doing (1)×a_1+(2) and simplifying, we get

$$F(x)<\frac{2a_1}{a_1-1}=4.$$

Define $b_1=4$. Similarly we get $G(x) < b_1$. Repeating the above steps, but reversing all the inequality signs, we can get

$$F(x)>\frac{2b_1}{b_1-1}=a_2,\quad G(x)>a_2,$$

$$F(x)<\frac{2a_2}{a_2-1}=b_2\quad and\quad G(x)<b_2.$$

This suggest defining

$$a_{n+1}=\frac{2b_n}{b_n-1}\quad and\quad b_n=\frac{2a_n}{a_n-1}$$

for $n=1,2,3,\ldots$. Replacing a_1, b_1, a_2, b_2 by a_n, b_n, a_{n+1}, b_{n+1} and repeating the steps above, we can prove $a_n< F(x)$, $G(x) < b_n$ for $n=1,2,3,\ldots$ by induction on n. Next we will show a_n, b_n have same limit. Now

$$a_{n+1}=\frac{2b_n}{b_n-1}=\frac{4a_n/(a_n-1)}{(a_n+1)/(a_n-1)}=\frac{4a_n}{a_n+1}.$$

Taking reciprocal, we get

$$\frac{1}{a_{n+1}}=\frac{1}{4}+\frac{1}{4}\frac{1}{a_n}.$$

Defining $c_n=1/a_n$, we get $c_{n+1}=(1+c_n)/4$. Subtracting 1/3 from both sides, we get $c_{n+1}-1/3 = (c_n-1/3)/4$. Using this, we get

$$c_{n+1}-\frac{1}{3}=\frac{1}{4^n}(c_1-\frac{1}{3})=\frac{1}{6\cdot 4^n}.$$

From this, letting n tends to infinity, we can see c_n has limit 1/3. Then a_n has limit 3. Similarly b_n has limit 3. Thus, for all $x>0$, $F(x)=3=G(x)$, i.e. $f(x)=3/x=g(x)$. Plugging these into the given equations, we see indeed they are solutions.

Olympiad Corner

(continued from page 1)

Problem 3. (*Cont.***)** Can "2" immediately to the right of the inequality be replaced by a smaller positive number?

Problem 4. In $\triangle ABC$, $AB > AC$, M is the midpoint of BC of its circumcircle containing A. Its incircle with incentre I is tangent to BC at D. The line passing through D and parallel to AI intersects the incircle again at P. Prove that the lines AP and IM intersect at a point on the circumcircle of $\triangle ABC$.

Primes in Arithmetic Progressions

(continued from page 2)

Assume there are integers x, y, z satisfying $x^n+y^n=z^n$ with $xyz\neq 0$ and $\gcd(n,xyz)=1$. Then $\gcd(p,x) = \gcd(p,y) = \gcd(p,z) = 1$. Let $w = x^{(p-1)/2}$. By Euler's theorem, $w^2=x^{p-1}\equiv 1 \pmod{p}$. Then p divides $w-1$ or $w+1$. Hence $x^{(p-1)/2}= w\equiv \pm 1 \pmod{p}$. Then $x^n \equiv \pm 1 \pmod{p}$. Similarly, y^n, $z^n \equiv \pm 1 \pmod{p}$. But then $x^n +y^n \equiv 0$ or $\pm 2 \pmod{p}$, contradicting $x^n+y^n=z^n$.

<u>Explanations for Facts 1 to 4.</u>

For fact 1, let $n=\min\{a,b\}$. For $n=1$,we may assume $a\geq b=1$ and take $(r,s)=(0,1)$. Suppose cases $n=1$ to k are true. For case $n=k+1$, say $a\geq b=k+1$. Dividing a by b, we can write $a=qb+c$, where $q=[a/b]$ and $0\leq c<b$. If $c=0$, then take $(r,s) = (1,q-1)$ to get $ar+bs = b = \gcd(a,b)$. If $c\geq 1$, then since $k+1=b>c\geq 1$ and $\gcd(b,c) = \gcd(b,a-qb) = \gcd(b,a)$, we can apply inductive step to get r', s' so that $\gcd(b,c)=br'+cs'$. Then $\gcd(a,b) = br'+(a-qb)s'= as'+b(r'-qs')$.

<u>Remark</u>: In case $\gcd(a,b)=1$, fact 1 gives $ar \equiv 1 \pmod{b}$. We denote this r by a^{-1} in (mod b). Hence we can cancel a in $ax \equiv ay \pmod{b}$ to get $x \equiv y \pmod{b}$ by multiplying both sides by a^{-1}.

For fact 2, let $k= \varphi(n)$ and let r_1, r_2, …, r_k be the integers in $[1,n]$ relatively prime to n. If $\gcd(a,n)=1$, then $ar_i \equiv ar_j \pmod{n}$ implies $r_i=r_j$ by the remark above. Then $ar_1,ar_2, \ldots,ar_k$ is just a permutation of $r_1, r_2, \ldots, r_k \pmod{n}$. So $(ar_1)(ar_2)\cdots(ar_k) \equiv r_1r_2 \cdots r_k \pmod{n}$. As $\gcd(r_1r_2 \cdots r_k,n)=1$, by the remark above we may cancel $r_1r_2 \cdots r_k$ to get $a^k \equiv 1 \pmod{n}$, which is Euler's theorem.

For fact 3, let $K= k_1k_2\cdots k_n$ and $M_i =K/k_i$. Then $\gcd(M_i,k_i) =1$ and for $j\neq i$, $M_j \equiv 0 \pmod{k_i}$. Let x be the integer in the interval $[1,K]$ such that

$$x\equiv c_1M_1^{\varphi(k_1)}+\cdots+c_nM_n^{\varphi(k_n)}\pmod{K}.$$

Using Euler's theorem, $x\equiv c_i \pmod{k_i}$. If x' in $[1,K]$ is another solution, then $x-x'\equiv c_i-c_i =0 \pmod{k_i}$ for $i=1,2,\cdots,n$. This leads to $x-x'\equiv 0 \pmod{K}$. As x, x' are both in $[1,K]$, we get $x=x'$.

For fact 4, $p=2$ or 3 cases are clear. For $p>3$, let a be in $[1, p-1]$. If $a\equiv a^{-1} \pmod{p}$, then $a^2\equiv 1 \pmod{p}$. So p divides $(a-1)(a+1)$. Hence $a=1$ or $p-1$. For a in $[2,p-2]$, we can form $(p-3)/2$ pairs a and a^{-1}. Then $(p-1)! \equiv 1(aa^{-1})^{(p-3)/2}(-1) = -1 \pmod{p}$.