THE UNIVERSITY OF TORONTO
UNDERGRADUATE MATHEMATICS COMPETITION

In Memory of Robert Barrington Leigh

March 9, 2013

Time: $3\frac{1}{2}$ hours

`No aids or calculators permitted.`

The grading is designed to encourage only the stronger students to attempt more than five problems. Each solution is graded out of 10. If the sum of the scores for the solutions to the five best problems does not exceed 30, this sum will be the final grade. If the sum of these scores does exceed 30, then all solutions will be graded for credit.

1. (a) Let a be an odd positive integer exceeding 3, and let n be a positive integer. Prove that

$$a^{2^n} - 1$$

has at least $n + 1$ distinct prime divisors.

(b) When $a = 3$, determine all the positive integers n for which the assertion in (a) is false.

2. ABCD is a square; points U and V are situated on the respective sides BC and CD. Prove that the perimeter of triangle CUV is equal to twice the sidelength of the square if and only if $\angle UAV = 45°$.

3. Let $f(x)$ be a convex increasing realvalued function defined on the closed interval $[0, 1]$ for which $f(0) = 0$ and $f(1) = 1$. Suppose that $0 < a < 1$ and that $b = f(a)$.

(a) Prove that f is continuous on $(0, 1)$.

(b) Prove that

$$0 \leq a - b \leq 2 \int_0^1 (x - f(x))dx \leq 1 - 4b(1 - a).$$

Notes. $f(x)$ is *increasing* if and only if $f(u) \leq f(v)$ whenever $u \leq v$, and is *convex* if and only if

$$f((1 - t)u + tv) \leq (1 - t)f(u) + tf(v)$$

whenever $0 < t < 1$.

4. Let S be the set of integers of the form $x^2 + xy + y^2$, where x and y are integers.

(a) Prove that any prime p in S is either equal to 3 or is congruent to 1 modulo 6.

(b) Prove that S includes all squares.

(c) Prove that S is closed under multiplication.

5. A point on an ellipse is joined to the ends of its major axis. Prove that the portion of a directrix intercepted by the two joining lines subtends a right angle at the corresponding focus.

Notes. The *directrix* corresponding to a focus F of an ellipse is a line with the property that, for any point P on the ellipse, the distance from P to F divided by the distance from P to the directrix is a constant e, called the *eccentricity*, less than 1. The major axis is the chord of the ellipse that passes through the two foci.

Please turn over. The are more questions overleaf.

6. Let $p(x) = x^4 + ax^3 + bx^2 + cx + d$ be a polynomial with rational coefficients. Suppose that $p(x)$ has exactly one real zero r. Prove that r is rational.

7. Let $(V, \langle \cdot \rangle)$ be a two-dimensional inner product space over the complex field $\mathbf{C}$ and let z_1 and z_2 be unit vectors in V. Prove that
$$\sup\{|\langle z, z_1\rangle\langle z, z_2\rangle| : \|z\| = 1\} \geq \frac{1}{2}$$
with equality if and only if $\langle z_1, z_2\rangle = 0$.

Note: The inner product $\langle z, w\rangle$ is linear in the left variable and satisfies $\langle w, z\rangle = \overline{\langle z, w\rangle}$. Also, $\|z\|^2 = \langle z, z\rangle$.

8. For any real square matrix A, the adjugate matrix, adj A, has as its elements that cofactors of the transpose of A, so that
$$A \cdot \text{adj } A = \text{adj } A \cdot A = (\det A)I \ .$$

(a) Suppose that A is an invertible square matrix. Show that
$$(\text{adj } (A^{\mathbf{t}}))^{-1} = (\text{adj } (A^{-1}))^{\mathbf{t}} \ .$$

(b) Suppose that adj $(A^{\mathbf{t}})$ is orthogonal (*i.e.*, its inverse is its transpose). Prove that A is invertible.

(c) Let A be an invertible $n \times n$ square matrix and let $\det\,(tI - A) = t^n + c_1 t^{n-1} + \cdots + c_{n-1}t + c_n$ be the characteristic polynomial of the matrix A. Determine the characteristic polynomial of adj A.

Note. A real square matrix M is *orthogonal* if and only if the product of M and its transpose $M^{\mathbf{t}}$ is the identity matrix.

9. Let S be a set upon whose elements there is a binary operation $(x, y) \rightarrow xy$ which is associative (*i.e.* $x(yz) = (xy)z$). Suppose that there exists an element $e \in S$ for which $e^2 = e$ and that for each $a \in S$, there is at least one element b for which $ba = e$ and at most one element c for which $ac = e$. Prove that S is a group with this binary operation.

Note. A group G is a set with an associative binary operation that contains an identity element u for which, given any element $x \in G$, $xu = ux = x$ and there exists $y \in G$ for which $yx = xy = u$.

10. (a) Let f be a real-valued function defined on the real number field $\mathbb{R}$ for which $|f(x) - f(y)| < |x - y|$ for any pair (x, y) of distinct elements of $\mathbb{R}$. Let $f^{(n)}$ denote the nth composite of f defined by $f^{(1)}(x) = f(x)$ and $f^{(n+1)}(x) = f(f^{(n)}(x))$ for $n \geq 2$. Prove that exactly one of the following situations must occur:

(i) $\lim_{n\rightarrow+\infty} f^{(n)}(x) = +\infty$ for each real x;

(ii) $\lim_{n\rightarrow+\infty} f^{(n)}(x) = -\infty$ for each real x;

(iii) there is a real number z such that
$$\lim_{n\rightarrow+\infty} f^{(n)}(x) = z$$
for each real x.

(b) Give examples to show that each of the three cases in (a) can occur.

Solutions

1. Let a be an odd positive integer exceeding 3, and let n be a positive integer. Prove that

$$a^{2^n} - 1$$

has at least $n+1$ distinct prime divisors.

(b) When $a = 3$, determine all the positive integers n for which the assertion in (a) is false.

Solution 1. (a) For $n = 1$, note that $a^2 - 1 = uv$, where $u = a - 1$ and $v = a + 1$. Since u and v are consecutive even integers, one of them is the product of 2 and an odd integer. Thus, $a^2 - 1$ has at least two prime divisors. We complete the proof by induction. Suppose it holds for the exponent n. Observe that

$$a^{2^n} - 1 = (a^{2^{n-1}} + 1)(a^{2^{n-1}} - 1).$$

The second factor on the right, by the induction hypothesis, has at least n distinct prime divisors. The first factor, being congruent to 2 modulo 4, must have an odd divisor exceeding 1. Any odd prime that divides the first factor cannot divide the second, and so there must be at least $n+1$ prime factors in all.

(b) Observe that $3^2 - 1 = 2^3$, $3^{2^2} - 1 = 3^4 - 1 = 2^4 \times 5$,

$$3^{2^3} - 1 = (3^4 - 1)(3^4 + 1) = (2^4 \times 5) \times (2 \times 41) = 2^5 \times 5 \times 41$$

and

$$3^{2^4} - 1 = (3^8 - 1)(3^8 + 1) = (2^5 \times 5 \times 41) \times (2 \times 17 \times 193) = 2^6 \times 5 \times 17 \times 41 \times 193.$$

By induction, as in (a), it can be shown that $3^{2^n} - 1$ has $n+1$ distinct prime factors when $n \geq 4$. It has exactly n primes factors when $n = 1, 2, 3$.

Solution 2. (J. Love) (a) Observe that, for each positive integer n,

$$a^{2^n} - 1 = (a-1)(a+1)(a^2+1)\ldots(a^{2^{n-1}} + 1).$$

This quantity is divisible by 2. Since a is odd, $a^2 \equiv 1 \bmod 4$, so that the last $n-1$ terms of the product on the right is equal to twice an odd integer, and therefore has at least one odd prime divisor. Since $a > 3$, at least one of $a - 1$ and $a + 1$ is equal to twice an odd prime.

It remains to show that no two of the factors on the right side can be divisible by the same odd prime. If p is an odd prime divisor of $a - 1$, then each of the remaining factors is congruent to 2 modulo p, If $i < j$ and p divides $a^{2^i} + 1$ and $a^{2^j} + 1$, then, since $a^{2^i} + 1$ divides $a^{2^j} - 1$, then so does p. But then p divides $2 = (a^{2^j} + 1) - (a^{2^j} - 1)$, which is false. Therefore, $a^{2^n} - 1$ is divisible by 2 and n odd primes, distinct divisors of $a^2 - 1$ and $a^{2^i} + 1$ for $1 \leq i \leq n-1$.

(b) As in (a), we can prove that 2 divides $N \equiv 3^{2^n} - 1$ and that distinct odd primes divide each of the $n-1$ factors $3^2 + 1$, $3^4 + 1$, $\cdots$, $3^{2^{n-1}+1}$ of N. Thus, there are at least n distinct primes dividing N. However, $3^{2^3} + 1 = 6562 = 2 \times 193$ is divisible by 2 odd primes, so that, when $n \geq 4$, N is divisible by $n+1$ distinct primes. However, since $3^2 - 1 = 2^3$, $3^4 - 1 = 2^4 \times 5$ and $3^8 - 1 = 6560 = 2^5 \times 5 \times 41$, the assertion in (a) fails for $a = 3$ and $n = 1, 2, 3$.

2. ABCD is a square; points U and V are situated on the respective sides BC and CD. Prove that the perimeter of triangle CUV is equal to twice the sidelength of the square if and only if $\angle UAV = 45°$.

Solution 1. (Y. Babich; J. Song) Produce CD to W so that $DW = BU$. Then triangles ABU and ADW are congruent (SAS) so that $BU = DW$.

First, assume that $\angle UAV = 45^\circ$. Then

$$\begin{aligned}\angle VAW &= \angle VAD + \angle DAW = \angle VAD + \angle BAU \\ &= 90^\circ - \angle UAV = 45^\circ.\end{aligned}$$

Since also $AU = AW$ and AV is common, triangles UAW and WAV are congruent (SAS) and $UV = VW = DV + BU$.

Therefore

$$CU + CV + UW = (CU + BU) + (CV + DV) = BC + CD$$

as desired.

On the other hand, assume that $CU + CV + UV = BC + CD$. Then

$$UV = (BC - CU) + (CD - CV) = BU + VD = VW,$$

so that triangles AUV and AWV are congruent (SSS) and $\angle UAV = \angle WAV = \angle VAD + \angle UAB$. Since $\angle UAB + \angle UAV + \angle VAD = 90^\circ$, it follows that $\angle UAV = 45^\circ$.

Solution 2. Let the side length of the square be 1, $|BU| = u$, $|DV| = v$, $|UV| = w$. Then $|CU| = 1 - u$ and $|CV| = 1 - v$.

Suppose that $\angle UAV = 45^\circ$. Since $45^\circ = \angle BAU + \angle DAV$,

$$1 = \tan 45^\circ = \frac{u+v}{1-uv},$$

whereupon $1 - uv = u + v$ and $1 + u^2v^2 = u^2 + 4uv + v^2$. By the Law of Cosines,

$$\begin{aligned}w^2 &= (1+u^2) + (1+v^2) - \sqrt{2(1+u^2)(1+v^2)} \\ &= u^2 + v^2 + 2 - \sqrt{2(1+u^2v^2+u^2+v^2)} = u^2 + v^2 + (2 - \sqrt{4(u^2+2uv+v^2)} \\ &= u^2 + v^2 + 2(1-(u+v)) = u^2 + v^2 + 2uv = (u+v)^2.\end{aligned}$$

. Hence $w = u + v$ and the perimeter of CUV is equal to $(1-u) + (1-v) + (u+v) = 2$.

On the other hand, suppose that $|UV| = u + v$. Then, by Pythagoras' Theorem,

$$u^2 + 2uv + v^2 = (1 - 2u + u^2) + (1 - 2v + v^2)$$

so that $u + v = 1 - uv$. Therefore

$$\tan(\angle UAB + \angle VAD) = \frac{u+v}{1-uv} = 1,$$

so that $\angle UAB + \angle VAD = 45^\circ$ and $\angle UAV = 45^\circ$.

Solution 3. (Z. Liu) Let $A \sim (0,0)$, $B \sim (1,0)$, $C \sim (1,1)$, $D \sim (0,1)$, $U \sim (1,u)$, and $V \sim (v,1)$, where $0 < u, v < 1$. Since

$$\cos \angle UAV \cdot |AU| \cdot |AV| = \overrightarrow{AU} \cdot \overrightarrow{AV},$$

$$\begin{aligned}\angle UAV = 45^\circ &\Leftrightarrow \sqrt{2}(u+v) = \sqrt{1+u^2}\sqrt{1+v^2} \\ &\Leftrightarrow (u+v)^2 = u^2 + 2uv + v^2 = 1 - 2uv + u^2v^2 = (1-uv)^2 \\ &\Leftrightarrow u + v = 1 - uv \Leftrightarrow (1-u)^2 + (1-v)^2 = (u+v)^2 \\ &\Leftrightarrow |UV| = |BU| + |VD| \\ &\Leftrightarrow |CU| + |CV| + |UV| = |BU| + |CU| + |CV| + |VD| = |BC| + |CD|.\end{aligned}$$

The result follows.

Solution 4. (J. Zung) Let U be fixed on BC. Then as V moves from C to D, the lengths of CV and UV strictly increase, so that the perimeter of triangle CUV strictly increases from $2CU < BC + CD$ to $CU+UD+CD > BC+CD$. Therefore, there is a unique position of V such that $CU+CV+UV = BC+CD$.

Also, as V moves from C to D, the angle UAV strictly increases from an angle less than 45° to an angle greater than 45°. Therefore, there is a unique position of V such that $\angle UAV = 45^\circ$. We need to show that the position of V is the same in both situations.

Select V so that UV is tangent to the circle with centre A that passes through B and D. Let T be the point of tangency. Then

$$CU + CV + VU = CU + CV + VT + TU = CU + CV + VD + UB = CD + CB.$$

Also, $\angle VAT = \frac{1}{2}\angle DAT$ and $\angle UAT = \frac{1}{2}\angle BAT$, so that $\angle UAV = 45^\circ$. Thus the point V is the unique point for both of the foregoing situations, and the desired result follows.

Solution 5. (partial: S. Rumsey) Suppose $\angle AUV = 45^\circ$. Let the image of B reflected in AU be E and the image of D reflected in AV be F. Then

$$\angle EAU + \angle FAV = \angle BAU + \angle DAV = 45^\circ = \angle UAC,$$

so that E annd F must fall on the same line through A. Since $AE = AB = AD = AF$, then $E = F$.

Also,

$$\angle AEU = \angle ABU = 90^\circ = \angle ADV = \angle AEV,$$

so that U, E, V are collinear and E lies on UV. Therefore

$$CU + CV + UV = CU + CV + UE + EV = CU + CV + BU + DV = BC + CD,$$

as desired.

3. Let $f(x)$ be a convex increasing realvalued function defined on the closed interval $[0, 1]$ for which $f(0) = 0$ and $f(1) = 1$. Suppose that $0 < a < 1$ and that $b = f(a)$.

   (a) Prove that f is continuous on $(0, 1)$.

   (b) Prove that

$$0 \le a - b \le 2\int_0^1 (x - f(x))dx \le 1 - 4b(1 - a).$$

   Notes. $f(x)$ is *increasing* if and only if $f(u) \le f(v)$ whenever $u \le v$, and is *convex* if and only if

$$f((1 - t)u + tv) \le (1 - t)f(u) + tf(v)$$

   whenever $0 < t < 1$.

Solution 1. (a) Let $x < y \le 1$. Then $y = (1 - t)x + t$ where $t = (y - x)/(1 - x)$ and $f(y) \le (1 - t)f(x) + tf(1)$. Therefore

$$0 \le f(y) - f(x) \le t[f(1) - f(x)] = \left[\frac{y - x}{1 - x}\right][1 - f(x)].$$

If follows that $\lim_{y\downarrow x} f(y) = f(x)$ so that f is right continuous at x. A similar argument shows that f is left continuous when $0 < x \le 1$. Therefore f is continuous on $[0, 1]$.

(b) Let $0 < x < 1$. Then $f(x) \leq (1-x)f(0) + xf(1) = x$, so that the graph of $y = f(x)$ over $[0,1]$ lies below the graph of $y = x$. Thus $a \geq b$.

Let $O = (0,0)$, $I = (1,1)$, $P = (a,b)$ and $Q = (a,a)$. The area between the graphs of $y = f(x)$ and $y = x$ is not less than the combined areas of the triangles OPQ and IPQ, namely $\frac{1}{2}(a-b)a + \frac{1}{2}(a-b)(1-a) = \frac{1}{2}(a-b)$. Therefore

$$\int_0^1 (x - f(x))dx \geq \frac{1}{2}(a-b).$$

The rightmost inequality is equivalent to $\int_0^1 f(x)dx \geq 2b(1-a)$. We first show that there is a line of equation $y = m(x-a) + b$ passing through (a,b) that passes under the graph of $y = f(x)$.

Suppose that $0 \leq u < x < v \leq 1$. Then

$$(v-x)f(x) + (x-u)f(x) = (v-u)f(x) \leq (v-x)f(u) + (x-u)f(v).$$

This is equivalent to

$$\frac{f(x) - f(u)}{x - u} \leq \frac{f(v) - f(x)}{v - x}.$$

Let m be any number between the supremum of the left side over u and the infimum of the right side over v.

The line $y = m(x-a) + b$ contains the points $(a - b/m, 0)$ and $(1, m(1-a) + b)$. By the convexity of f, it cannot contain any point of the graph of $y = f(x)$so lies underneath the graph. The area under the line is equal to

$$\frac{1}{2}\left[\left(1 - a + \frac{b}{m}\right)(m(1-a) + b)\right] = \frac{2}{m}\left[\frac{m(1-a) + b}{2}\right]^2 \geq 2b(1-a).$$

This gives the desired result.

Solution 2 to part of (b). First, we have that $b = f(a) \leq (1-a)f(0) + af(1) = a$, so that $a - b \geq 0$. Making use of the respective substitutions $x = ta$ and $x = (1-t)a + t = a + t(1-a)$ we find that

$$\begin{aligned}\int_0^a (x - f(x))dx &= a\int_0^1 (ta - f(ta))dt \geq a\int_0^1 (ta - tf(a))dt \\ &= a\int_0^1 t(a-b)dt = \frac{a(a-b)}{2},\end{aligned}$$

and that

$$\begin{aligned}\int_a^1 (x - f(x))dx &= (1-a)\int_0^1 [(1-t)a + t - f((1-t)a + t)]dt \\ &\geq (1-a)\int_0^1 [(1-t)a + t - ((1-t)f(a) + tf(1))]dt \\ &= (1-a)\int_0^1 (1-t)(a-b) = \frac{(1-a)(a-b)}{2}.\end{aligned}$$

Adding these two inequalities together yields

$$\int_0^1 (x - f(x))dx \geq \frac{a-b}{2}.$$

4. Let S be the set of integers of the form $x^2 + xy + y^2$, where x and y are integers.

   (a) Prove that any prime p in S is either equal to 3 or is congruent to 1 modulo 6.

   (b) Prove that S includes all squares.

(c) Prove that S is closed under multiplication.

Solution. (a) Let $f(x,y) = x^2 + xy + y^2$. Then $3 = f(1,1)$ is representable. It is straightforward to establish that 2 is not representable. (If $x^2 + xy + y^2 = 2$, then $(2x+y)^2 + 3y^2 = 8$.) Let p be a prime exceeding 3 for which $p = f(u,v)$ for some integers u and v. Then, modulo 3,

$$0 \not\equiv p \equiv 4p = 4(u^2 + uv + v^2) = (2u+v)^2 + 3v^2 \equiv (2u+v)^2 \equiv 1 .$$

Since p is odd, the result follows. (Alternatively, modulo 3, we have that $0 \not\equiv p = (u-v)^2 + 3uv \equiv (u-v)^2 \equiv 1$.)

(b) Observe that $a^2 = f(a,0) = f(a,-a)$ for each integer a.

(c) Observe that $x^2 + xy + y^2 = (x - y\omega)(x - y\omega^2)$, where ω is an imaginary cube root of unity, *i.e.*, $1 + \omega + \omega^2 = 0$ (this can be deduced from the factorization of $x^3 - y^3$ into linear factors over $\mathbb{C}$). Then, since $\omega^2 = -1 - \omega$ and $\omega^3 = 1$.

$$\begin{aligned}(x^2 + xy + y^2)(u^2 + uv + v^2) &= [(x - y\omega)(x - y\omega^2)][(u - v\omega)(u - v\omega^2)]\\ &= [(x - y\omega)(u - v\omega)][(x - y\omega^2)(u - v\omega^2)]\\ &= [(xu - (xv + yu)\omega + yv\omega^2][(xu - (xv + yu)\omega^2 + yv\omega]\\ &= [(xu - yv) - (xv + yu + yv)\omega][(xu - yv) - (xv + yu + yv)\omega^2].\end{aligned}$$

It is readily checked that

$$f(x,y)f(u,v) = f(xu - yv, xv + yu + yv).$$

5. A point on an ellipse is joined to the ends of its major axis. Prove that the portion of a directrix intercepted by the two joining lines subtends a right angle at the corresponding focus.

Notes. The *directrix* corresponding to a focus F of an ellipse is a line with the property that, for any point P on the ellipse, the distance from P to F divided by the distance from P to the directrix is a constant e, called the eccentricity, less than 1. The major axis is the chord of the ellipse that passes through the two foci.

Solution 1. Suppose that the focus is at the origin of the Cartesian plane, the directrix is the line $x = 1$ and the eccentricity of the ellipse is e. Then the equation of the ellipse is $\sqrt{x^2 + y^2} = e(1 - x)$, or

$$y^2 = -(1 - e^2)x^2 - 2e^2x + e^2 \ .$$

The major axis is the $x-$axis and the ellipse intersects this axis at the points $(e/(1+e), 0)$ and $(-e/(1-e), 0)$. Let (u,v) be an arbitrary point on the ellipse. Then the lines determined by the point (u,v) and these endpoints respectively intersect the directrix at

$$\left(1, \frac{v}{(1+e)u - e}\right) \qquad \text{and} \qquad \left(1, \frac{v}{(1-e)u + e}\right) .$$

The product of the slopes of the segments joining these to the origin is

$$\frac{v^2}{(1 - e^2)u^2 + [e(1+e) - e(1-e)]u - e^2} = \frac{-(1 - e^2)u^2 - 2e^2u + e^2}{(1 - e^2)u^2 + 2e^2u - e^2} = -1.$$

Solution 2. (J. Song; T. Xiao) Let the equation of the ellipse by $x^2/a^2 + y^2/b^2 = 1$ and the point $P \sim (u,v)$. The right directrix of the ellipse has equation $x = a^2/c$ and the right focus F is at $(c,0)$, where $a^2 = b^2 + c^2$.

The equation of the line through $(-a,0)$ and P is $(u+a)y = v(x+a)$ and this meets the directrix at the point

$$G \sim \left(\frac{a^2}{c}, \frac{av(a+c)}{c(u+a)}\right).$$

The equation of the line through $(a, 0)$ and P is $(u-a)y = v(x-a)$ and this meets the directric at the point

$$H \sim \left(\frac{a^2}{c}, \frac{av(a-c)}{c(u-a)} \right).$$

Let K be the point $(a^2/c, 0)$ where the directrix and major axis intersect. Because P lies on the ellipse, we have that $a^2v^2 = b^2(a^2 - u^2)$.

There are two possible ways to proceed. Taking the dot product of the vectors $\overrightarrow{FG}$ and $\overrightarrow{FH}$, we obtain that

$$\begin{aligned} \left(\frac{a^2}{c} - c, \frac{av(a+c)}{c(u+a} \right) \cdot \left(\frac{a^2}{c} - c, \frac{av(a-c)}{c(u-a} \right) &= \frac{1}{c^2} \left[(a^2-c^2)^2 - \frac{a^2v^2(a^2-c^2)}{a^2-u^2} \right] \\ &= \frac{a^2-c^2}{c^2}[a^2 - c^2 - b^2] = 0, \end{aligned}$$

so that $\angle GFH = 90°$.

Alternatively, we can use the Law of Cosines to obtain that

$$\begin{aligned} 2|GF||HF| \cos \angle GFH &= |FG|^2 + |GK|^2 - |GH^2 \\ &= 2|FK|^2 + |GK|^2 + |HK|^2 - (|GK| + |HK|)^2 \\ &= 2[|FK|^2 - |GK||HK|] \\ &= 2\left[\left(\frac{a^2}{c} - c \right)^2 - \frac{a^2v^2(a^2-c^2)}{c^2(a^2-u^2)} \Big) \right] \\ &= \frac{2}{c^2}[(a^2-c^2)^2 - b^2(a^2-c^2)] = \frac{2(a^2-c^2)}{c^2}[a^2-c^2-b^2] = 0, \end{aligned}$$

from which the result follows. (Note that $|u-a| = a-u$ since $u < a$.)

6. Let $p(x) = x^4 + ax^3 + bx^2 + cx + d$ be a polynomial with rational coefficients. Suppose that $p(x)$ has exactly one real root r. Prove that r is rational.

Solution. Since nonreal roots occur in pairs, $p(x)$ must have an even number of real roots counting multiplicity. Therefore r must be a double or quadruple root. If r is a quadruple root, then $p(x) = (x-r)^4$ and $r = -a/4$ is rational. Suppose, otherwise, that $p(x) = (x-r)^2q(x)$ where $q(x)$ is an irreducible quadratic. The derivative $p'(x)$ is equal to $(x-r)f(x)$ where $f(x) = 2q(x) + (x-r)q'(x)$. Since $q(r)$ does not vanish, $f(r) \neq q(r)$ so that $f(x)$ and $q(x)$ must be distinct and coprime. The monic greatest common divisor of $p(x)$ and $p'(x)$ must therefore $x - r$. Since (by the Euclidean algorithm) this is a polynomial with rational coefficients, therefore r is rational.

7. Let $(V, \langle \cdot \rangle)$ be a two-dimensional inner product space over the complex field $\mathbf{C}$ and let z_1 and z_2 be unit vectors in V. Prove that

$$\sup\{|\langle z, z_1 \rangle \langle z, z_2 \rangle| : \|z\| = 1\} \geq \frac{1}{2}$$

with equality if and only if $\langle z_1, z_2 \rangle = 0$.

Note: The inner product $\langle z, w \rangle$ is linear in the left variable and satisfies $\langle w, z \rangle = \overline{\langle z, w \rangle}$. Also, $\|z\|^2 = \langle z, z \rangle$.

Solution. Let $\langle z_1, z_2 \rangle = a + bi$ for real a and b. Since $|\langle z, z_1 \rangle \langle z, z_2 \rangle| = |\langle z, z_2 \rangle \langle z, -z_2 \rangle|$, there is no loss of generality in assuming that $a = \text{Re}\langle z_1, z_2 \rangle \geq 0$. Suppose that $w = (z_1 + z_2)/(\|z_1 + z_2\|$. Then $\|w\| = 1$ and the supremum in the problem is not less than $\|\langle w, z_1 \rangle \langle w, z_2 \rangle\|$. Note that $|\langle w, z_1 \rangle| = |1 + \langle z_2, z_1 \rangle|/(\|z_1 + z_2\|)$ and that $|\langle w, z_2 \rangle| = |1 + \langle z_1, z_2 \rangle|/(\|z_1 + z_2\|)$. Also $\|z_1 + z_2\| = \langle z_1 + z_2, z_1 + z_2 \rangle = \langle z_1, z_1 \rangle + \langle z_2, z_2 \rangle +$

$\langle z_1, z_2\rangle + \langle z_2, z_1\rangle = 2 + 2\text{Re}\langle z_1, z_2\rangle = 2 + 2a$.

$$\begin{aligned}|\langle w, z_1\rangle\langle w, z_2\rangle| &= \frac{|1+\langle z_1, z_2\rangle|^2}{2+2a} \\ &= \frac{(1+a)^2+b^2}{2(1+a)} \\ &= \frac{1}{2}\left(1+a+\frac{b^2}{1+a}\right) \geq \frac{1}{2},\end{aligned}$$

with equality if and only if $a = b = 0$, *i.e.* $\langle z_1, z_2\rangle = 0$. Thus, if the supremum of $\frac{1}{2}$, then $\langle z_1, z_2\rangle = 0$.

On the other hand, suppose that $\langle z_1, z_2\rangle = 9$. Then $\{z_1, z_2\}$ is an orthonormal basis, and we can write $z = uz_1 + vz_2$ where $|u|^2 + |v|^2 = 1$ for $\|z\| = 1$. Then

$$|\langle z, z_1\rangle\langle z, z_2\rangle| = |u||v| \leq \frac{1}{2}(|u|^2+|v|^2) = \frac{1}{2}$$

with equality if and only if $|u| = |v| = 2^{-1/2}$. Therefore, the supremum is $\frac{1}{2}$ in this case.

Comment. If V is a real, rather than complex, vetor space, then a trigonometric solution is possible. Wolog, we can assume that a basis has been selected so that $z_1 = (1, 0)$ and $z_2 = (\cos\theta, \sin\theta)$. Suppose that $z = (\cos\phi, \sin\phi)$, then

$$\begin{aligned}\langle z, z_1\rangle\langle z, z_2\rangle &= \cos\phi(\cos\theta\cos\phi + \sin\theta\sin\phi) = \cos\phi(\cos(\theta-\phi)) \\ &= \frac{1}{2}[\cos\theta + \cos(\theta - 2\phi)].\end{aligned}$$

If $\cos\theta = 0$ and $\sin\theta = \pm 1$, then the value of this expression is $|\frac{1}{2}\cos(\theta-2\phi)| \leq \frac{1}{2}$, so that the supremum is equal to $1/2$, attainable when $2\phi = \theta$.

On the other hand, when $\cos\theta > 0$ and $2\phi = \theta$, the expression is greater than $1/2$ and the supremum exceeds $1/2$. Similarly, when $\cos\theta < 0$, and $2\phi = \theta + \pi$, the expression is less than $-1/2$ and again the supremum exceeds $1/2$.

8. For any real square matrix A, the adjugate matrix, adj A, has as its elements the cofactors of the transpose of A, so that

$$A \cdot \text{adj } A = \text{adj } A \cdot A = (\det A)I\ .$$

(a) Suppose that A is an invertible square matrix. Show that

$$(\text{adj }(A^{\mathbf{t}}))^{-1} = (\text{adj }(A^{-1}))^{\mathbf{t}}\ .$$

(b) Suppose that adj $(A^{\mathbf{t}})$ is orthogonal (*i.e.*, its inverse is its transpose). Prove that A is invertible.

(c) Let A be an invertible $n \times n$ square matrix and let det $(tI - A) = t^n + c_1t^{n-1} + \cdots + c_{n-1}t + c_n$ be the characteristic polynomial of the matrix A. Determine the characteristic polynomial of adj A.

Solution. (a) Since $A^{\mathbf{t}}\text{adj }(A^{\mathbf{t}}) = (\det A)I$ and $A^{-1}(\text{adj }(A^{-1})) = (\det A)^{-1} \cdot I$, it follows that

$$(\text{adj }(A^{\mathbf{t}}))^{-1} = \frac{1}{\det A}A^{\mathbf{t}} = (\text{adj }(A^{-1}))^{\mathbf{t}}.$$

(b) Since adj $(A^{\mathbf{t}}) \cdot (\text{adj }(A^{\mathbf{t}}))^{\mathbf{t}} = I$, then

$$A^{\mathbf{t}} = A^{\mathbf{t}}\text{adj }(A^{\mathbf{t}})(\text{adj }A^{\mathbf{t}})^{\mathbf{t}} = (\det A)(\text{adj }A^{\mathbf{t}})^{\mathbf{t}}.$$

Since $A \neq O$, det $A \neq 0$.

(c)

$$\begin{aligned}\det\,(tI - \text{adj } A) &= \frac{1}{\det A}\cdot \det\,(tA - A \text{ adj } A) = \frac{1}{\det A}\cdot\det\,(tA - (\det A)I)\\ &= \frac{(-t)^n}{\det A}\cdot\det\left(\frac{\det A}{t}I - A\right)\\ &= \frac{(-t)^n}{(-1)^n c_n}\left(\sum_{k=0}^{n}\left(\frac{(-1)^n c_n}{t}\right)^{n-k} c_k\right)\\ &= \sum_{k=0}^{n}(-1)^{n(n-k)}c_k c_n^{n-k-1}t^k,\end{aligned}$$

with $c_0 = 1$.

9. Let S be a set upon whose elements there is a binary operation $(x, y) \rightarrow xy$ which is associative (*i.e.* $x(yz) = (xy)z$). Suppose that there exists an element $e \in S$ for which $e^2 = e$ and that for each $a \in S$, there is at least one element b for which $ba = e$ and at most one element c for which $ac = e$. Prove that S is a group with this binary operation.

   Note. A group G is a set with an associative binary operation that contains an indentity element u for which, given any element $x \in G$, $xu = ux = x$ and there exists $y \in G$ for which $yx = xy = u$.

Solution 1. We show that e is the identity element of S and that each element of S has a two-sided inverse. Let t be an arbitrary element of S. There is an element $s \in S$ for which $st = e$. Hence $e = e^2 = s(tst)$. Since also $st = e$, we must have that $t = tst = te$. Therefore e is a right identity in S.

Suppose that $r \in S$ is such that $rs = e$. Then $et = rst = re = r$ (since e is a right identity). Therefore $ets = rs = e$. Since $ee = e$ as well, $e = ts$ and so $et = tst = t$.

Solution 2. (J. Love) Let $a \in S$. There exists b such that $ba = e$. Therefore, $b(ae) = (ba)e = e^2 = e$, so that $a = ae$ ($\forall a \in S$). We have that $e = ba = (be)a = b(ea)$ whereupon $a = ea$. Hence e is a two-sided identity.

Suppose that $ba = e$. Select $d \in S$ so that $db = e$. Then $d = de = d(ba) = (db)a = ea = a$, so that a is a two-sded inverse of b.

This is problem #4504 from the *American Mathematical Monthly* **54** (1961), 54.

10. Let f be a real-valued function defined on the real number field $\mathbf{R}$ for which $|f(x) - f(y)| < |x - y|$ for any pair (x, y) of distinct elements of $\mathbf{R}$. Let $f^{(n)}$ denote the nth composite of f defined by $f^{(1)}(x) = f(x)$ and $f^{(n+1)}(x) = f(f^{(n)}(x)$ for $n \geq 2$. Prove that exactly one of the following situations must occur:

    (i) $\lim_{n\rightarrow+\infty} f^{(n)} = +\infty$ for each real x;

    (ii) $\lim_{n\rightarrow+\infty} f^{(n)} = -\infty$ for each real x;

    (iii) there is a real number z such that

    $$\lim_{n\rightarrow+\infty} f^{(n)}(x) = z$$

    for each real x.

    (b) Give examples to show that each of the three cases in (a) can occur.

Solution. (a) Note that the condition on f implies that f is uniformly continuous. Suppose that there exists a real number z for which $f(z) = z$. Let $x \neq z$. Then $|f(x) - f(z)| = |f(x) - z| < |x - z|$. If $f^{(n)}(x) < z$ for each positive integer n, then $\{f^{(n)}(x)\}$ is an increasing sequence that converges to a real number $w \leq z$.

Since $w = \lim f^{(n+1)}(x) = \lim f(f^{(n)}(x)) = f(w)$ and since $|f(w) - f(z)| = |z - w|$, we must have $z = w$. In a similar way, it can be shown that $\lim f^{(n)}(x) = z$ when $f^{(n)}(x) \geq z$ for each n.

The remaining possibility is that $\{f^{(n)}(x)\}$ can be partitioned into two subsequences, one increasing to a limit $u \leq z$ and the other decreasing to a limit $v \geq z$. Suppose, if possible, that $u \neq z$. Since $|f(u) - f(z)| < |u - z|$, for each integer n, we must have either $f^{(n)}(x) \leq u$ or $f^{(n)}(x) \geq z$. Suppose, if possible, that $z < f(u) < v$. Because f is continuous, there exits $\epsilon > 0$ for which $|t - u| \leq \epsilon$ implies that $z < f(t) < v$. But for some integer m, $u - \epsilon < f^{(m)}(x) \leq u$ so that $z < f^{(m+1)}(x) < v$, an impossibility. Since $f(u)$ cannot equal u, then $f(u) \geq v$ so that

$$|v - z| = v - z \leq f(u) - f(z) < |u - z| = z - u.$$

If $v \neq z$, then it can be similarly shown that $|u - z| < |v - z|$. Since $|u - z| < |v - z|$ and $|u - z| > |v - z|$ are incompatible, one of $u = z$ and $v = z$ must hold. But when one of these holds, then so must the other and the result follows.

Suppose that there is no z for which $f(z) = z$. Then the function $g(x) = f(x) - x$ is continuous and vanishes nowhere on $\mathbf{R}$. If $g(x) > 0$ for all x, then for each x, $f^{(n)}(x)$ is an increasing sequence. It cannot have a finite limit, since this limit would be a fixpoint of f. Therefore the sequence must diverge to infinity. The case that $g(x) < 0$ for all x can be similarly handled.

(b) (i) Let $f(x) = (1 + x^2)^{1/2}$. Then $f(x) > x$ and so $f^{(n)}(x)$ is a strictly increasing function of n. Since $f'(x) = x(1 + x^2)^{-1/2}$, we find that, given x, y, there exists a number z for which

$$|f(x) - f(y)| = |f'(z)||x - y| < |x - y|.$$

(ii) Let $f(x) = -(1 + x^2)^{1/2}$.

(iii) Let $f(x) = \frac{1}{2}x$.