## Junior problems

J271. Find all positive integers $n$ with the following property: if $a, b, c$ are integers such that $n$ divides $a b+b c+c a+1$, then $n$ divides $a b c(a+b+c+a b c)$.

Proposed by Titu Andreescu, University of Texas at Dallas and Gabriel Dospinescu, Ecole Polytechnique, Lyon, France

## Solution by the authors

We will prove that all positive divisors of 720 are solutions of the problem. If $n$ is a solution, then by choosing $a=3, b=5, c=-2$ (for which $a b+b c+c a+1=0$ ) we obtain $n \mid 720$. Conversely, let $d$ be a divisor of 720 and suppose that $d$ divides $a b+b c+c a+1$. We want to prove that $d$ divides $a b c(a+b+c+a b c)$. We may assume that $d$ is a power of a prime. The key ingredient is the following identity

$$
\left(a^{2}-1\right)\left(b^{2}-1\right)\left(c^{2}-1\right)=(a+b+c+a b c)^{2}-(a b+b c+c a+1)^{2} .
$$

This follows easily by multiplying the equalities

$$
(a+1)(b+1)(c+1)=a b c+a+b+c+a b+b c+c a+1
$$

and

$$
(a-1)(b-1)(c-1)=a b c+a+b+c-(a b+b c+c a+1) .
$$

Define $f(a, b, c)=a^{2} b^{2} c^{2}\left(a^{2}-1\right)\left(b^{2}-1\right)\left(c^{2}-1\right)$. If at least two of the numbers $a, b, c$ are odd, then $f(a, b, c)$ is a multiple of $4 \cdot 64=256$. Hence if $2^{k}$ divides $a b+b c+c a+1$ and $1 \leq k \leq 4$, then at least two of the numbers $a, b, c$ are odd and the previous discussion yields $2^{2 k} \mid a^{2} b^{2} c^{2}(a+b+c+a b c)^{2}$, hence $2^{k} \mid a b c(a+b+c+a b c)$. A similar argument shows that if $3^{k} \mid a b+b c+c a+1$ and $1 \leq k \leq 2$, then 27 divides $f(a, b, c)$, hence $3^{2 k-1}$ divides $(a b c(a+b+c+a b c))^{2}$ and then $3^{k} \mid a b c(a+b+c+a b c)$. Finally, suppose that 5 divides $a b+b c+c a+1$ and 5 does not divide $a b c(a+b+c+a b c)$. The previous identity shows that $a, b, c$ are each congruent to 2 or $3 \bmod 5$ and one can easily check that this contradicts the fact that 5 divides $a b+b c+c a+1$.

Also solved by Polyahedra, Polk State College, FL, USA.

J272. Let $A B C$ be a triangle with centroid $G$ and circumcenter $O$. Prove that if $B C$ is its greatest side, then $G$ lies in the interior of the circle of diameter $A O$.

Proposed by Ivan Borsenco, Massachusetts Institute of Technology, USA

Solution by Ercole Suppa, Teramo, Italy


Let $a=B C, b=C A, c=A B$, let $M$ the midpoint of $B C$, let $D$ be the second intersection point between $A M$ and the circumcircle of $\triangle A B C$.

By the Power of Point theorem, we have $A M \cdot M D=B M \cdot M C$. Thus, we get

$$
A D=A M+M D=m_{a}+\frac{\frac{a}{2} \cdot \frac{a}{2}}{m_{a}}=\frac{4 m_{a}^{2}+a^{2}}{4 m_{a}}=\frac{2 b^{2}+2 c^{2}}{4 m_{a}}=\frac{b^{2}+c^{2}}{2 m_{a}}
$$

Now, taking into account that the circle of diameter $A O$ is the locus of midpoints of chords of $(O)$ that that pass through $A$, we have that $G$ lies in the interior of the circle of diameter $A O$ if and only if $A G<A D / 2$ or equivalently

$$
\frac{2}{3} m_{a}<\frac{1}{2} \cdot \frac{b^{2}+c^{2}}{2 m_{a}} \quad \Leftrightarrow \quad 8 m_{a}^{2}<3\left(b^{2}+c^{2}\right) \quad \Leftrightarrow \quad b^{2}+c^{2}<2 a^{2}
$$

Since $B C$ is the greatest side of $\triangle A B C$, the last inequality holds, so we are done.
Also solved by YoungSoo Kwon, St. Andrew's School, Delaware, USA; Daniel Lasaosa, Universidad Pública de Navarra, Spain; Polyahedra, Polk State College, FL, USA.

J273. Let $a, b, c$ be real numbers greater than or equal to 1 . Prove that

$$
\frac{a^{3}+2}{b^{2}-b+1}+\frac{b^{3}+2}{c^{2}-c+1}+\frac{c^{3}+2}{a^{2}-a+1} \geq 9 .
$$

Proposed by Titu Andreescu, University of Texas at Dallas, USA

Solution by Daniel Lasaosa, Universidad Pública de Navarra, Spain
Note first that $a^{3}+2 \geq 3\left(a^{2}-a+1\right)$ is equivalent to $a^{3}-3 a^{2}+3 a-1=(a-1)^{3} \geq 0$, clearly true by hypothesis and with equality iff $a=1$. Analogous inequalities hold for $b, c$. Therefore, application of the AM-GM produces

$$
\begin{gathered}
\frac{a^{3}+2}{b^{2}-b+1}+\frac{b^{3}+2}{c^{2}-c+1}+\frac{c^{3}+2}{a^{2}-a+1} \geq \\
\geq 3 \sqrt[3]{\frac{a^{3}+2}{a^{2}-a+1} \cdot \frac{b^{3}+2}{b^{2}-b+1} \cdot \frac{c^{3}+2}{c^{2}-c+1}} \geq 3 \sqrt[3]{3^{3}}=9
\end{gathered}
$$

The conclusion follows, and the necessary condition for equality $a=b=c=1$ is clearly also sufficient.
Also solved by Zarif Ibragimov, SamSU, Samarkand, Uzbekistan; Polyahedra, Polk State College, FL, USA; f; Arber Igrishta, Eqrem Qabej, Vushtrri, Kosovo; Arkady Alt, San Jose, California, USA; Ercole Suppa, Teramo, Italy; Mathematical Group "Galaktika shqiptare", Albania; Harun Immanuel, ITS Surabaya; Jonathan Luke Lottes, The College at Brockport, State University of New York; Prithwijit De, HBCSE, Mumbai, India; Sayan Das, Indian Statistical Institute, Kolkata; Paolo Perfetti, Università degli studi di Tor Vergata Roma, Roma, Italy; Shivang Jindal, Jaipur, India; Alessandro Ventullo, Milan, Italy; Ioan Viorel Codreanu, Satulung, Maramures, Romania.

J274. Let $p$ be a prime and let $k$ be a nonnegative integer. Find all positive integer solutions $(x, y, z)$ to the equation

$$
x^{k}(y-z)+y^{k}(z-x)+z^{k}(x-y)=p .
$$

Proposed by Alessandro Ventullo, Milan, Italy

First solution by Polyahedra, Polk State College, USA
Let $A_{k}=x^{k}(y-z)+y^{k}(z-x)+z^{k}(x-y)$. Then for $k=0,1, A_{k} \equiv 0$, so no solution exists. Suppose that $k \geq 2$. Then

$$
\begin{aligned}
A_{k} & =(y-z)\left(x^{k}-y^{k}\right)+(x-y)\left(z^{k}-y^{k}\right)=(x-y)(y-z) \sum_{i=1}^{k-1}\left(x^{i}-z^{i}\right) y^{k-1-i} \\
& =(x-y)(y-z)(x-z) B_{k},
\end{aligned}
$$

where

$$
B_{k}=\sum_{i=1}^{k-1}\left(\sum_{j=0}^{i-1} x^{j} z^{i-1-j}\right) y^{k-1-i}=\sum_{i+j+l=k-2} x^{i} y^{j} z^{l}
$$

Now for $k \geq 3, B_{k}$ is an integer greater than 2 , so no solution to $A_{k}=p$ is possible. Finally, for $k=2$, $A_{k}=(x-y)(y-z)(x-z)=p$ if and only if $p=2$ and $(x, y, z)=(n+2, n+1, n),(n, n+2, n+1)$, or $(n+1, n, n+2)$ for $n \geq 1$.

Second solution by Polyahedra, Polk State College, USA
Note that

$$
A_{k}=x^{k}(y-z)+y^{k}(z-x)+z^{k}(x-y)=-\left|\begin{array}{ccc}
x & x^{k} & 1 \\
y & y^{k} & 1 \\
z & z^{k} & 1
\end{array}\right|
$$

which is twice the area of $\triangle X Y Z$, where $X=\left(x, x^{k}\right), Y=\left(y, y^{k}\right), Z=\left(z, z^{k}\right)$, and $X Y Z$ is in the clockwise orientation. Clearly, $A_{k} \equiv 0$ for $k=0,1$. Assume that $k \geq 2$ and $x>y>z$. By Pick's theorem, $A_{k}=2\left(I_{k}-\frac{1}{2} B-1\right)$, where $I_{k}$ and $B$ are the numbers of lattice points in the interior and on the boundary of $\triangle X Y Z$, respectively. Since the slopes of $X Y, Y Z$, and $Z X$ are integers, it is easy to see that $B=2(x-z)$, thus $A_{k}=2\left(I_{k}+x-z-1\right)$. Therefore, for $A_{k}=p$, we must have $p=2, x-z=2$, and $I_{k}=0$. Now $\frac{1}{2}\left[(z+2)^{k}+z^{k}\right] \geq(z+1)^{k}+1$, with equality if and only if $k=2$. So $W=\left(y, y^{k}+1\right)$ is an interior point of $\triangle X Y Z$ for $k \geq 3$. Finally, it is easy to see that when $k=2$, the solutions are $(x, y, z)=(n+2, n+1, n)$, $(n, n+2, n+1)$, or $(n+1, n, n+2)$ for $n \geq 1$.

Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain.

J275. Let $A B C D$ be a rectangle and let point $E$ lie on side $A B$. The circle through $A, B$, and the orthogonal projection of $E$ onto $C D$ intersects $A D$ and $B C$ at $X$ and $Y$. Prove that $X Y$ passes through the orthocenter of triangle $C D E$.

Proposed by Titu Andreescu, University of Texas at Dallas, USA

First solution by Ercole Suppa, Teramo, Italy


Let $F$ be the orthogonal projection of $E$ onto $C D$, let $H=E F \cap X Y, K=D H \cap C E$.
Clearly $X Y \| A B$ so $D X H F$ is cyclic. Thus a simple angle chasing gives

$$
\begin{align*}
\angle E D H & =\angle E D C-\angle H D C=\angle F A B-\angle H D C= \\
& =\angle F X B-\angle F X Y=\angle Y X B \tag{1}
\end{align*}
$$

From cyclic quadrilaterals $A B F X$ and $E B C F$ we get

$$
\begin{gather*}
\angle D E F=\angle D A F=\angle X A F=\angle X B F  \tag{2}\\
\angle F E C=\angle F B C \tag{3}
\end{gather*}
$$

By using (1),(2),(3) we obtain

$$
\begin{aligned}
\angle D K E & =180^{\circ}-\angle E D K-\angle D E K= \\
& =180^{\circ}-\angle E D H-\angle D E F-\angle F E C= \\
& =180^{\circ}-\angle Y X B-\angle X B F-\angle F B C= \\
& =180^{\circ}-\angle Y X B-\angle X B Y= \\
& =\angle X Y B=90^{\circ}
\end{aligned}
$$

Therefore $D K \perp E C$. Since $E F \perp D C$ and $H=D K \cap E F$, it follows that $H$ is the orthocenter of $\triangle C D E$, as we wanted to prove.

Second solution by Cosmin Pohoata, Princeton University, USA As in the previous solution, let $F$ be the orthogonal projection of $E$ onto $C D$ and let $H$ be the intersection of $E F$ with $X Y$. It is well-known that the reflections of the orthocenter of a triangle across is sidelines lie on the circumcircle of the triangle. Thus, $H$ is the orthocenter of $C D E$ if and onl only if $F C \cdot F D=F E \cdot F H$. But as before $X Y \| A B$, so
$F C \cdot F D=X H \cdot H Y$. On the other hand, if $F^{\prime}$ is the second intersection of $F E$ with the circumcircle of $F A B$, the power of $H$ with respect to $(F A B)$ yields $F^{\prime} H \cdot F H=X H \cdot X Y$; hence, it follows that $F C \cdot F D=F^{\prime} H \cdot F H$. However, $F E=F^{\prime} H$, by symmetry, so, we get $F C \cdot F D=F E \cdot F H$, as desired.

Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain; YoungSoo Kwon, St. Andrew's School, Delaware, USA; Polyahedra, Polk State College, USA.

J276. Find all positive integers $m$ and $n$ such that

$$
10^{n}-6^{m}=4 n^{2}
$$

Proposed by Tigran Akopyan, Vanadzor, Armenia

Solution by Alessandro Ventullo, Milan, Italy
It is easy to see that if $n=1$, then $m=1$ and $(1,1)$ is a solution to the given equation. We prove that this is the only solution. Assume that $n>1$ and $n$ odd. Then, $10^{n}-6^{m} \equiv-6^{m}(\bmod 8)$ and $4 n^{2} \equiv 4$ $(\bmod 8)$ and it is clear that $-6^{m} \equiv 4(\bmod 8)$ if and only if $m=2$. But $10^{n}>36+4 n^{2}$ for all positive integers $n>1$, therefore there are no solutions when $n$ is odd. Let $n$ be an even number, i.e. $n=2 k$ for some $k \in \mathbb{Z}^{+}$. Hence,

$$
\left(10^{k}-4 k\right)\left(10^{k}+4 k\right)=6^{m} .
$$

Since there are no solutions for $k=1,2$, let us assume that $k>2$. Clearly $m \geq 4$ and simplifying by 2 , we get

$$
\begin{equation*}
\left(2^{k-2} \cdot 5^{k}-k\right)\left(2^{k-2} \cdot 5^{k}+k\right)=2^{m-4} \cdot 3^{m} . \tag{1}
\end{equation*}
$$

If $k$ is odd, then $m=4$. But $2^{k-2} \cdot 5^{k}+k \geq 2 \cdot 5^{3}+3>3^{4}$, contradiction. Therefore, $k$ must be even. Assume that $k=2^{\alpha} h$, where $\alpha, h \in \mathbb{Z}^{+}$and $h$ is odd. If $\alpha \geq k-2$, then $2^{k-2} \mid k$, which implies that $2^{k-2} \leq k$. This gives $k=3,4$ and an easy check shows that there are no solutions for this values. If $\alpha<k-2$, then equation (1) becomes

$$
2^{2 \alpha}\left(2^{k-2-\alpha} \cdot 5^{k}-h\right)\left(2^{k-2-\alpha} \cdot 5^{k}+h\right)=2^{m-4} \cdot 3^{m}
$$

and by unique factorizaton we have $2 \alpha=m-4$. Therefore, from the inequality $k>\alpha+2$, we obtain $n>2 \alpha+4=m$. But this implies that $10^{n}=6^{m}+4 n^{2}<6^{n}+4 n^{2}$, which is false for all integers $n>1$. Hence, there are no solutions for $n$ even and the statement follows.

Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain;Polyahedra, Polk State College, USA; Arbër Avdullahu,Mehmet Akif College,Kosovo; David Xu; G. C. Greubel, Newport News, VA; Mathematical Group "Galaktika shqiptare", Albania; Harun Immanuel, ITS Surabaya; Toan Pham Quang, Dang Thai Mai Secondary School, Vinh, Vietnam; Tony Morse and Oiza Ochi, College at Brockport, State University of New York.

## Senior problems

S271. Determine if there is an $n \times n$ square with all entries cubes of pairwise distinct positive integers such that the product of entries on each of the $n$ rows, $n$ columns, and two diagonals is $2013^{2013}$.

Proposed by Titu Andreescu, University of Texas at Dallas, USA

Solution by Li Zhou, Polk State College, USA
Shown below is De Morgan's $11 \times 11$ additive magic square, where the sum of entries on each of the 11 rows, 11 columns, and two diagonals is $(1+2+\cdots+121) / 11=671$.

| 56 | 117 | 46 | 107 | 36 | 97 | 26 | 87 | 16 | 77 | 6 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 7 | 57 | 118 | 47 | 108 | 37 | 98 | 27 | 88 | 17 | 67 |
| 68 | 8 | 58 | 119 | 48 | 109 | 38 | 99 | 28 | 78 | 18 |
| 19 | 69 | 9 | 59 | 120 | 49 | 110 | 39 | 89 | 29 | 79 |
| 80 | 20 | 70 | 10 | 60 | 121 | 50 | 100 | 40 | 90 | 30 |
| 31 | 81 | 21 | 71 | 11 | 61 | 111 | 51 | 101 | 41 | 91 |
| 92 | 32 | 82 | 22 | 72 | 1 | 62 | 112 | 52 | 102 | 42 |
| 43 | 93 | 33 | 83 | 12 | 73 | 2 | 63 | 113 | 53 | 103 |
| 104 | 44 | 94 | 23 | 84 | 13 | 74 | 3 | 64 | 114 | 54 |
| 55 | 105 | 34 | 95 | 24 | 85 | 14 | 75 | 4 | 65 | 115 |
| 116 | 45 | 106 | 35 | 96 | 25 | 86 | 15 | 76 | 5 | 66 |

Raising $2013^{3}$ to each entry of the the table, we obtain an $11 \times 11$ multiplicative magic square satisfying the requirements.

S272. Let $A_{1}, A_{2}, \ldots, A_{2 n}$ be a polygon inscribed in a circle $C(O, R)$. Diagonals $A_{1} A_{n+1}, A_{2} A_{n+2}, \ldots, A_{n} A_{2 n}$ intersect at point $P$. Let $G$ be the centroid of the polygon. Prove that $\angle O P G$ is acute.

Proposed by Ivan Borsenco, Massachusetts Institute of Technology, USA

Solution by Li Zhou, Polk State College, USA


For $1 \leq i \leq n$, let $M_{i}$ be the midpoint of $A_{i} A_{n+i}$. Then $O M_{i} \perp A_{i} A_{n+i}$, so the $n$-gon $M_{1} M_{2} \cdots M_{n}$ is circumscribed by the circle $C^{\prime}$ of diameter $O P$. Since $G$ is also the centroid of $M_{1} M_{2} \cdots M_{n}$, it must be in the interior of $C^{\prime}$. Hence, $\angle O P G$ is acute.

Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain.

S273. Let $a, b, c$ be positive integers such that $a \geq b \geq c$ and $\frac{a-c}{2}$ is a prime. Prove that if

$$
a^{2}+b^{2}+c^{2}-2(a b+b c+c a)=b
$$

then $b$ is either a prime or a perfect square.
Proposed by Titu Andreescu, University of Texas at Dallas, USA

Solution by Stephanie Lash and Jessica Schuler, College at Brockport, State University of New York
We rewrite the equation as $(a-c)^{2}=b(1-b+2 a+2 c)$, from which we have immediately that $b \mid(a-c)^{2}$, i.e. $b \left\lvert\, 4\left(\frac{a-c}{2}\right)^{2}\right.$.

We will consider two cases. First, suppose $\frac{a-c}{2}=2$. This means that $b \mid 16$ and so $b \in\{1,2,4,8,16\}$. To complete the problem in this case we need to show that $b \neq 8$. Suppose that $b=8$. The rewritten equation becomes $16=8(1-8+2 a+2 c)$ iff $2=2 a+2 c-7$, which is a contradiction because the left hand side is even while the right hand side is odd. Now, suppose that $\frac{a-c}{2}$ is an odd prime. Among other things this implies that $a-c \neq 0$ and it is possible to cancel it if needed. The divisors of $4\left(\frac{a-c}{2}\right)^{2}$ are

$$
1,2,4, \frac{a-c}{2}, a-c, 2(a-c), \frac{(a-c)^{2}}{4}, \frac{(a-c)^{2}}{2},(a-c)^{2}
$$

To complete the problem in this case we need to show that

$$
b \notin\left\{a-c, 2(a-c), \frac{(a-c)^{2}}{2}\right\}
$$

Suppose that $b=a-c$. The rewritten equation becomes

$$
(a-c)^{2}=(a-c)(1-a+c+2 a+2 c) \Longleftrightarrow a-c=1+a+3 c \Longleftrightarrow 0=1+3 c
$$

a contradiction. Suppose that $b=2(a-c)$. Then

$$
(a-c)^{2}=2(a-c)(1-2 a+2 c+2 a+2 c) \Longleftrightarrow a-c=2+8 c \Longleftrightarrow a=2+9 c
$$

In the same time, $b=2(a-c)=4+16 c>2+9 c=a$, which is a contradiction. Finally, suppose that $b=\frac{(a-c)^{2}}{2}$. Then, since $a-c$ is even, $b$ is also even and

$$
(a-c)^{2}=\frac{(a-c)^{2}}{2}(1-b+2 a+2 c) \Longleftrightarrow 1=\frac{1}{2}(1-b+2 a+2 b) \Longleftrightarrow 1=2 a+2 c-b
$$

which is a contradiction because the left hand side is odd while the right hand side is even. This completes the proof.

Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain; Li Zhou, Polk State College, USA; Alessandro Ventullo, Milan, Italy.

S274. Let $a, b, c$ be positive real numbers such that $a b c=1$. Prove that

$$
\frac{a}{c a+1}+\frac{b}{a b+1}+\frac{c}{b c+1} \leq \frac{1}{2}\left(a^{2}+b^{2}+c^{2}\right) .
$$

Proposed by Sayan Das, Kolkata, India

Solution by Ercole Suppa, Teramo, Italy
We make the well-known substitution $a=\frac{x}{y}, b=\frac{y}{z}$ and $c=\frac{z}{x}$, where $x, y, z>0$. The original inequality becomes:

$$
\begin{equation*}
\frac{2 x}{y+z}+\frac{2 y}{z+x}+\frac{2 z}{x+y} \leq \frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}} \tag{*}
\end{equation*}
$$

According to AM-GM inequality we get

$$
\begin{equation*}
\frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}}=\frac{1}{2}\left(\frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}\right)+\frac{1}{2}\left(\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}}\right)+\frac{1}{2}\left(\frac{z^{2}}{x^{2}}+\frac{x^{2}}{y^{2}}\right) \geq \frac{x}{z}+\frac{y}{x}+\frac{z}{y} \tag{1}
\end{equation*}
$$

From AM-GM and Cauchy Schwarz inequalities we obtain

$$
\begin{align*}
\frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}} & =\sqrt{\frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}}} \cdot \sqrt{\frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}}} \\
& \geq \sqrt{3} \cdot \sqrt{\frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}}} \geq \frac{x}{y}+\frac{y}{z}+\frac{z}{x} \tag{2}
\end{align*}
$$

Summing up the inequalities (1),(2) we deduce that

$$
\begin{equation*}
\frac{x^{2}}{y^{2}}+\frac{y^{2}}{z^{2}}+\frac{z^{2}}{x^{2}} \geq \frac{1}{2}\left(\frac{x}{y}+\frac{x}{z}\right)+\frac{1}{2}\left(\frac{y}{x}+\frac{y}{z}\right)+\frac{1}{2}\left(\frac{z}{x}+\frac{z}{y}\right) \tag{3}
\end{equation*}
$$

Applying the AM-HM inequality for two numbers, we obtain

$$
\begin{align*}
\frac{1}{2}\left(\frac{x}{y}+\frac{x}{z}\right)+\frac{1}{2}\left(\frac{y}{x}+\frac{y}{z}\right)+\frac{1}{2}\left(\frac{z}{x}+\frac{z}{y}\right) & \geq \frac{2}{\frac{y+z}{x}}+\frac{2}{\frac{x+z}{y}}+\frac{2}{\frac{x+y}{z}}= \\
& =\frac{2 x}{y+z}+\frac{2 y}{x+z}+\frac{2 z}{x+y} \tag{4}
\end{align*}
$$

Finally, from (3) and (4), we get $\left({ }^{*}\right)$ which is exactly the desired result.
Also solved by Georgios Batzolis, Mandoulides High School, Thessaloniki, Greece; Daniel Lasaosa, Universidad Pública de Navarra, Spain; AN- anduud Problem Solving Group, Ulaanbaatar, Mongolia; Ioan Viorel Codreanu, Satulung, Maramures, Romania; Li Zhou, Polk State College, USA; Arkady Alt, San Jose ,California, USA; Mathematical Group "Galaktika shqiptare", Albania; Paolo Perfetti, Università degli studi di Tor Vergata Roma, Roma, Italy; Zarif Ibragimov, SamSU, Samarkand, Uzbekistan.

S275. Let $A B C$ be a triangle with incircle $\mathcal{I}$ and incenter $I$. Let $A^{\prime}, B^{\prime}, C^{\prime}$ be the intersections of $\mathcal{I}$ with the segments $A I, B I, C I$, respectively. Prove that

$$
\frac{A B}{A^{\prime} B^{\prime}}+\frac{B C}{B^{\prime} C^{\prime}}+\frac{C A}{C^{\prime} A^{\prime}} \geq 12-4\left(\sin \frac{A}{2}+\sin \frac{B}{2}+\sin \frac{C}{2}\right) .
$$

Proposed by Marius Stanean, Zalau, Romania

## Solution by Daniel Lasaosa, Universidad Pública de Navarra, Spain

## Lemma:

Clearly,

$$
\angle A^{\prime} I B^{\prime}=\angle A I B=180^{\circ}-\frac{A+B}{2}=90^{\circ}+\frac{C}{2},
$$

or $\angle A^{\prime} C^{\prime} B^{\prime}=45^{\circ}+\frac{C}{4}$, and applying the Sine Law, and that $r=4 R \sin \frac{A}{2} \sin \frac{B}{2} \sin \frac{C}{2}$, where $r, R$ are respectively the inradius and circunradius of $A B C$, we find

$$
\frac{A^{\prime} B^{\prime}}{A B}=\frac{r}{R} \frac{\sin \left(45^{\circ}+\frac{C}{4}\right)}{\sin C}=2 \sin \frac{A}{2} \sin \frac{B}{2} \frac{\sin \left(45^{\circ}+\frac{C}{4}\right)}{\cos \frac{C}{2}} .
$$

Now,

$$
2 \sin \frac{A}{2} \sin \frac{B}{2}=\cos \frac{A-B}{2}-\cos \frac{A+B}{2} \leq 1-\sin \frac{C}{2},
$$

with equality iff $A=B$, or denoting $\gamma=\frac{C}{4}+45^{\circ}$, we have $\sin \frac{C}{2}=-\cos \left(\frac{C}{2}+90^{\circ}\right)=-\cos (2 \gamma), \cos \frac{C}{2}=$ $\sin \left(\frac{C}{2}+90^{\circ}\right)=\sin (2 \gamma)$, and

$$
\frac{A^{\prime} B^{\prime}}{A B} \leq(1+\cos (2 \gamma)) \frac{\sin \gamma}{\sin (2 \gamma)}=\cos \gamma
$$

with equality iff $A=B$. Analogous relations may be found for the other terms in the LHS, defining $\alpha=\frac{A}{4}+45^{\circ}$ and $\beta=\frac{B}{4}+45^{\circ}$, yielding

$$
\frac{A B}{A^{\prime} B^{\prime}}+\frac{B C}{B^{\prime} C^{\prime}}+\frac{C A}{C^{\prime} A^{\prime}} \geq \frac{1}{\cos \alpha}+\frac{1}{\cos \beta}+\frac{1}{\cos \gamma}
$$

and using the definition of $\alpha, \beta, \gamma$ in the RHS of the proposed inequality, it suffices to show that

$$
\frac{1}{\cos \alpha}+\frac{1}{\cos \beta}+\frac{1}{\cos \gamma} \geq 8\left(\cos ^{2} \alpha+\cos ^{2} \beta+\cos ^{2} \gamma\right) .
$$

Note furthermore that, since $0<A<180^{\circ}$, we have $45^{\circ}<\alpha<90^{\circ}$, or $\alpha, \beta, \gamma$ are the angles of an acute triangle, or all cosines are positive reals. It is also well-known (or easily provable using the Cosine Law) that $\cos ^{2} \alpha+\cos ^{2} \beta+\cos ^{2} \gamma+2 \cos \alpha \cos \beta \cos \gamma=1$, or it suffices to show that

$$
\frac{1}{\cos \alpha}+\frac{1}{\cos \beta}+\frac{1}{\cos \gamma}+16 \cos \alpha \cos \beta \cos \gamma \geq 8
$$

clearly true after applying the AM-GM inequality to the sum in the LHS, and with equality iff $\alpha=\beta=\gamma=$ $60^{\circ}$, ie iff $A B C$ is equilateral, which is also clearly necessary and sufficient for the proposed inequality to become an equality. The conclusion follows.

Also solved by Stephanie Lash and Jessica Schuler, College at Brockport, State University of New York; Arkady Alt, San Jose ,California, USA; Li Zhou, Polk State College, USA.

S276. Let $a, b, c$ be real numbers such that

$$
\frac{2}{a^{2}+1}+\frac{2}{b^{2}+1}+\frac{2}{c^{2}+1} \geq 3
$$

Prove that $(a-2)^{2}+(b-2)^{2}+(c-2)^{2} \geq 3$.
Proposed by Titu Andreescu, University of Texas at Dallas, USA

Solution by Arkady Alt, San Jose, California, USA
Notice that

$$
\sum_{c y c} \frac{2}{a^{2}+1} \geq 3 \Longleftrightarrow \sum_{c y c}\left(\frac{2}{a^{2}+1}-1\right) \geq 0 \Longleftrightarrow \sum_{c y c} \frac{1-a^{2}}{1+a^{2}} \geq 0
$$

Now, the key part is to see that

$$
\begin{aligned}
(a-2)^{2}-\frac{2}{a^{2}+1} & =\frac{a^{4}-4 a^{3}+5 a^{2}-4 a+2}{a^{2}+1}=\frac{a^{4}-4 a^{3}+6 a^{2}-4 a+1+\left(1-a^{2}\right)}{a^{2}+1} \\
& =\frac{(a-2)^{4}}{a^{2}+1}+\frac{1-a^{2}}{1+a^{2}} .
\end{aligned}
$$

It follows that

$$
\sum_{c y c}(a-2)^{2}=\sum_{c y c} \frac{2}{a^{2}+1}+\sum_{c y c} \frac{(a-2)^{4}}{a^{2}+1}+\sum_{c y c} \frac{1-a^{2}}{1+a^{2}} \geq \sum_{c y c} \frac{2}{a^{2}+1} \geq 3 .
$$

Also solved by Zarif Ibragimov, SamSU, Samarkand, Uzbekistan; Mathematical Group "Galaktika shqiptare", Albania; Daniel Lasaosa, Universidad Pública de Navarra, Spain; AN-anduud Problem Solving Group, Ulaanbaatar, Mongolia; Li Zhou, Polk State College, USA.

## Undergraduate problems

U271. Let $a>b$ be positive real numbers and let $n$ be a positive integer. Prove that

$$
\frac{\left(a^{n+1}-b^{n+1}\right)^{n-1}}{\left(a^{n}-b^{n}\right)^{n}}>\frac{n}{(n+1)^{2}} \cdot \frac{e}{a-b}
$$

where $e$ is the Euler number.
Proposed by Ivan Borsenco, Massachusetts Institute of Technology, USA

## Solution by AN-anduud Problem Solving Group, Ulaanbaatar, Mongolia

Let us consider following function

$$
f(x)=(n-1) \log \left(x^{n}+x^{n-1}+\cdots+1\right)-n \log \left(x^{n-1}+x^{n-2}+\cdots+1\right)
$$

Taking the derivative respect with $x$, we have

$$
f^{\prime}(x)=\frac{(n-1)\left(n x^{n-1}+(n-1) x^{n-2}+\cdots+1\right)}{x^{n}+x^{n-1}+\cdots+1}-\frac{n\left((n-1) x^{n-2}+(n-2) x^{n-3}+\cdots+1\right)}{x^{n-1}+x^{n-2}+\cdots+1} .
$$

If we prove following inequality

$$
\begin{equation*}
(n-1)\left(\sum_{k=1}^{n} k x^{k-1}\right) \cdot\left(\sum_{k=1}^{n} x^{k-1}\right) \geq n\left(\sum_{k=1}^{n-1} k x^{k-1}\right) \cdot\left(\sum_{k=1}^{n+1} x^{k-1}\right) \tag{*}
\end{equation*}
$$

then for any $x$ with $x>1$ we have $f^{\prime}(x)>0$. Hence $f(x)$ is increasing on the open interval $(0, \infty)$.

$$
\begin{aligned}
\forall x>1: f(x)> & f(1) \Leftrightarrow \log \frac{\left(x^{n}+x^{n-1}+\cdots+1\right)^{n-1}}{\left(x^{n-1}+x^{n-2}+\cdots+1\right)^{n}} \geq \log \frac{(n+1)^{n-1}}{n^{n}} \\
& \frac{\left(x^{n}+x^{n-1}+\cdots+1\right)^{n-1}}{\left(x^{n-1}+x^{n-2}+\cdots+1\right)^{n}} \geq \frac{(n+1)^{n-1}}{n^{n}}
\end{aligned}
$$

Thus (1) inequality is proved. Now we will prove (*).

$$
\begin{gather*}
(*) \Leftrightarrow(n-1)\left(\sum_{k=1}^{n} k x^{k-1}\right)\left(x^{n}-1\right) \geq n\left(\sum_{k=1}^{n-1} k x^{k-1}\right)\left(x^{n+1}-1\right) \\
\Leftrightarrow(n-1) \sum_{k=1}^{n} k x^{n+k-1}+n \sum_{k=1}^{n-1} k x^{k-1} \geq n \sum_{k=1}^{n-1} k x^{n+k}+(n-1) \sum_{k=1}^{n} k x^{k-1} \\
\Leftrightarrow \sum_{k=1}^{n-1}(n-k) x^{n-1+k}+\sum_{k=1}^{n-1} \geq(n-1) n x^{n-1} \tag{**}
\end{gather*}
$$

Now we will use AM-GM inequality for $(n-1) n$ numbers.Then $(* *)$ is proved, so our lemma is proved. Let us solve the posed problem using our lemma.

$$
\begin{aligned}
\frac{\left(a^{n+1}-b^{n+1}\right)^{n-1}}{\left(a^{n}-b^{n}\right)^{n}} & =\frac{(a-b)^{n-1}\left(a^{n}+a^{n-1} b+\cdots+b^{n}\right)^{n-1}}{(a-b)^{n}\left(a^{n-1}+a^{n-2} b+\cdots+b^{n-1}\right)^{n}} \\
& =\frac{1}{a-b} \cdot \frac{\left(\left(\frac{a}{b}\right)^{n}+\left(\frac{a}{b}\right)^{n-1}+\cdots+1\right)^{n-1}}{\left(\left(\frac{a}{b}\right)^{n-1}+\left(\frac{a}{b}\right)^{n-2}+\cdots+1\right)^{n}} \\
& \stackrel{a}{b}=x>1 \\
= & \frac{1}{a-b} \cdot \frac{\left(x^{n}+x^{n-1}+\cdots+1\right)^{n-1}}{\left(x^{n-1}+x^{n-2}+\cdots+1\right)^{n}}
\end{aligned}
$$

by the lemma

$$
\geq \frac{1}{a-b} \cdot \frac{(n+1)^{n-1}}{n^{n}}=\frac{n}{(n+1)^{2}} \cdot \frac{1}{a-b} \cdot\left(1+\frac{1}{n}\right)^{n+1}
$$

using well known inequality $\left(1+\frac{1}{n}\right)^{n+1}>e$

$$
>\frac{n}{(n+1)^{2}} \cdot \frac{e}{a-b} .
$$

Hence our desired inequality is proved.
Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain; Arkady Alt, San Jose, California, USA; Paolo Perfetti, Università degli studi di Tor Vergata Roma, Roma, Italy; Jedrzej Garnek, Adam Mickiewicz University, Poznan, Poland.

U272. Let $a$ be a positive real number and let $\left(a_{n}\right)_{n \geq 0}$ be the sequence defined by $a_{0}=\sqrt{a}, a_{n+1}=\sqrt{a_{n}+a}$, for all positive integers $n$. Prove that there are infinitely many irrational numbers among the terms of the sequence.

Proposed by Marius Cavachi, Constanţa, Romania

Solution by Daniel Lasaosa, Universidad Pública de Navarra, Spain
Assume that the result is false. Then, either all terms in the sequence are rational, or there is a last irrational term $a_{N}$, and $a_{N+1}, a_{N+2}, \ldots$ are all rational. If two consecutive terms $a_{N+1}, a_{N+2}$ are rational, then $a=a_{N+2}^{2}-a_{N+1}$ must clearly be rational. Therefore, if $a_{N}$ is irrational, $a_{N+1}^{2}=a_{N}+a$ is irrational, and so is $a_{N+1}$, or if the proposed result is false, then $a$ is rational, and so is every term in the sequence.

From the previous argument, assuming that the proposed result is false, a positive rational $a$ exists such each $a_{n}$ is rational for all $n \geq 0$. Clearly $a_{1}=\sqrt{a+\sqrt{a}}>\sqrt{a}=a_{0}$, and if $a_{n}>a_{n-1}$, then $a_{n+1}=$ $\sqrt{a+a_{n}}>\sqrt{a+a_{n-1}}=a_{n}$, or by trivial induction the sequence is strictly increasing. Moreover, if $\sqrt{a}=\frac{u}{v}$ for $u, v$ coprime, an increasing sequence of integers $u_{n}$ exists such that $u_{0}=u$, and $u_{n+1}=\sqrt{u^{2}+u_{n} v}$. Indeed, with such a definition it follows that if $a_{n}=\frac{u_{n}}{v}$, then $a_{n+1}=\frac{u_{n+1}}{v}$. Moreover, since $a_{n+1}$ is rational, if $u_{n}$ is an integer, then $u_{n+1}$ is rational and at the same time the square root of an integer, hence an integer too, or since $u_{0}$ is an integer, then by trivial induction so is every $u_{n}=v a_{n}$, or the $u_{n}$ 's are a strictly increasing sequence of positive integers, hence unbounded. Or for sufficiently large $n, u_{n}$ will be as large as we desire, and at some point we will have $a_{n}=v u_{n}>\frac{1+\sqrt{1+4 a}}{2}$. Then,

$$
a<\frac{\left(2 a_{n}-1\right)^{2}-1}{4}=a_{n}^{2}-a_{n}, \quad a_{n+1}=\sqrt{a+a_{n}}<\sqrt{a_{n}^{2}}=a_{n},
$$

and the sequence would decrease, contradiction, hence the proposed result cannot be false. The conclusion follows.

U273. Let $\Phi_{n}$ be the $n$th cyclotomic polynomial, defined by

$$
\Phi_{n}(X)=\prod_{1 \leq m \leq n, \operatorname{gcd}(m, n)=1}\left(X-e^{\frac{2 i \pi m}{n}}\right) .
$$

a) Let $k$ and $n$ be positive integers with $k$ even and $n>1$. Prove that

$$
\pi^{k \varphi(n)} \cdot \prod_{p} \Phi_{n}\left(\frac{1}{p^{k}}\right) \in \mathbb{Q},
$$

where the product is taken over all primes and $\varphi$ is the Euler totient function.
b) Prove that

$$
\prod_{p}\left(1-\frac{1}{p^{2}}+\frac{1}{p^{6}}-\frac{1}{p^{8}}+\frac{1}{p^{10}}-\frac{1}{p^{14}}+\frac{1}{p^{16}}\right)=\frac{192090682746473135625}{3446336510402 \pi^{16}}
$$

Proposed by Albert Stadler, Herrliberg, Switzerland

Solution by Konstantinos Tsouvalas, University of Athens, Athens, Greece
a) We will use induction. First of all, we will use the following formula:

$$
\zeta(2 n)=(-1)^{n+1} \frac{B_{2 n}(2 \pi)^{2 n}}{2(2 n)!}
$$

where $\zeta$ denotes Riemann's function and $B_{2 n}$ the 2n-nth Bernoulli number.
For the cuclotomic polynomial it is known that:

$$
\begin{gathered}
\Phi_{n}(X)=(-1)^{\sum_{d \mid n} \mu(n / d)} \prod_{d \mid n}\left(1-X^{d}\right)^{\mu(n / d)}=\prod_{d \mid n}\left(1-X^{d}\right)^{\mu(n / d)} \\
\prod_{d \mid n}\left(1-X^{d}\right)^{\mu(n / d)}
\end{gathered}
$$

We also have:

$$
n=\sum_{d \mid n} \phi(d)
$$

hence from Mobius inversion formula:

$$
\phi(n)=\sum_{d \mid n} \mu\left(\frac{n}{d}\right) d
$$

Then:

$$
\begin{gathered}
\pi^{k \phi(n)} \prod_{p} \Phi_{n}\left(p^{-k}\right)=\pi^{k \phi(n)} \prod_{d \mid n}\left(\prod_{p}\left(1-\frac{1}{p^{k d}}\right)\right)^{\mu(n / d)} \\
=\prod_{d \mid n}\left(\pi^{k d} \prod_{p}\left(1-\frac{1}{p^{k d}}\right)\right)^{\mu(n / d)} \\
=\prod_{d \mid n}\left(\frac{(k d)!}{(-1)^{k d / 2+1} B_{k d^{2}} 2^{k d-1}}\right)^{\mu(n / d)} \in \mathbb{Q}
\end{gathered}
$$

b)We oserve that:

$$
\Phi_{15}\left(p^{-2}\right) \frac{\left(1-p^{-30}\right)\left(1-p^{-2}\right)}{\left(1-p^{-6}\right)\left(1-p^{-10}\right)}
$$

Finally we have:

$$
\pi^{16} \prod_{p} \Phi_{15}\left(p^{-2}\right)=\frac{\zeta(10) \zeta(6)}{\zeta(2) \zeta(30)}
$$

which is the desired number.
Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain; Jedrzej Garnek, Adam Mickiewicz University, Poznan, Poland.

U274. Let $A_{1}, \ldots, A_{m} \in M_{n}(\mathbb{C})$ satisfying $A_{1}+\cdots+A_{m}=m I_{n}$ and $A_{1}{ }^{2}=\cdots=A_{m}{ }^{2}=I_{n}$. Prove that $A_{1}=\cdots=A_{m}$.

Proposed by Marius Cavachi, Constanţa, Romania

Solution by Jedrzej Garnek, Adam Mickiewicz University, Poznan, Poland Note that since $A_{i}^{2}=I_{n}$, the eigenvalues of $A_{i}$ satisfy equation $\lambda^{2}=1$, i.e. all eigenvalues of $A_{i}$ are equal to $\pm 1$. Thus, since trace of a matrix is sum of its eigenvalues, $\operatorname{tr} A_{i} \leq n$, with equality iff all eigenvalues are equal to 1 .
On the other hand: $m n=\operatorname{tr} m I_{n}=\operatorname{tr}\left(A_{1}+\ldots+A_{m}\right)=\operatorname{tr} A_{1}+\ldots+\operatorname{tr} A_{m} \leq n+\ldots+n=m n$. Thus for all $i$ all eigenvalues of $A_{i}$ are equal to 1 .

Finally, since $A_{i}^{2}-I_{n}=0$, the minimal polynomial of $A_{i}$ divides $x^{2}-1$, and has no multiple roots, so that $A_{i}$ is diagonalizable. But the only diagonalizable $n \times n$ matrix with all eigenvalues equal to 1 is the identity matrix - thus $A_{i}=I_{n}$ for all $i$.

Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain; Nikolaos Zarifis, National Technical University of Athens, Athens, Greece; Moubinool Omarjee, Lycée Henri IV, Paris, France; Konstantinos Tsouvalas, University of Athens, Athens, Greece.

U275. Let $m$ and $n$ be positive integers and let $\left(a_{k}\right)_{k \geq 1}$ be real numbers. Prove that

$$
\sum_{d|m, e| n, g \mid \operatorname{gcd}(d, e)} \frac{\mu(g)}{g} d e \cdot a_{d e / g}=\sum_{k \mid m n} k a_{k}
$$

Here, $\mu$ is the usual Möbius function.
Proposed by Darij Grinberg, Massachusetts Institute of Technology, USA

Solution by Daniel Lasaosa, Universidad Pública de Navarra, Spain
Since the result is proposed for any sequence of real numbers, and $a_{k}$ only appears in the sum in the LHS when $\frac{d e}{g}=k$, then the proposed result is equivalently formulated as follows: given any positive integer $k$, for any pair of positive integers $m, n$ such that $m n$ is a multiple of $k$, we have

$$
\sum_{d|m, e| n, \left.\frac{d e}{k} \right\rvert\, \operatorname{gcd}(d, e)} \mu\left(\frac{d e}{k}\right)=1
$$

We prove the proposed result, expressed in this latter form, by induction on the number of distinct primes that divide simultaneously $m$ and $n$.

If $m, n$ are coprime, then so are $d, e$, and $\operatorname{gcd}(d, e)=1$, or $\frac{d e}{k}=1$, ie, there is exactly one term in the sum, occurring when $d=\operatorname{gcd}(k, m)$ and $e=\operatorname{gcd}(k, n)$, for which $\mu\left(\frac{d e}{k}\right)=\mu(1)=1$, and the result clearly follows in this case.

Let $p$ be a prime that divides $m, n$, with respective multiplicities $U, V \geq 1$. Let $t, u, v$ the multiplicities with which $p$ divides $k, d, e$, where clearly $u \in\{0,1, \ldots, U\}$ and $v \in\{0,1, \ldots, V\}$. The multiplicities of $p$ in $\frac{d e}{k}$ and $\operatorname{gcd}(d, e)$ are respectively $u+v-t$ and $\min (u, v)$. Since $k$ must divide de, but at the same time a nonzero contribution to the sum will happen iff $\frac{d e}{k}$ is square-free, we must have $u+v-t \in\{0,1\}$ for all nonzero contributions to the sum, while at the same time, since $\frac{d e}{k}$ divides $\operatorname{gcd}(d, e)$, we must have $u+v-t \leq \min (u, v)$, or equivalently $t \geq \max (u, v)$. The set of values that the pair $(u, v)$ can take therefore satisfies $\max (0, t-V) \leq u \leq \min (t, U)\}$ and $v=t-u$, or $\max (1, t+1-V) \leq u \leq \min (t, U)\}$ and $u=t+1-V$. Note therefore that there is always exactly one more pair $(u, v)$ such that $u+v-t=0$, than pairs such that $u+v-t=1$.

Denote now by $m^{\prime}, n^{\prime}, d^{\prime}, e^{\prime}, k^{\prime}$ the respective results of removing all factors $p$ from $m, n, d, e, k$. For each set $\left(m^{\prime}, n^{\prime}, d^{\prime}, e^{\prime}, k^{\prime}\right)$, consider all possible pairs $(u, v)$ as described above. For the pairs of the first kind, we have $\mu\left(\frac{d e}{k}\right)=\mu\left(\frac{d^{\prime} e^{\prime}}{k^{\prime}}\right)$, since $p$ does not appear in $\frac{d e}{k}$, while for the pairs of the second kind, we have $\mu\left(\frac{d e}{k}\right)=\mu\left(p \frac{d^{\prime} e^{\prime}}{k^{\prime}}\right)=-\mu\left(\frac{d^{\prime} e^{\prime}}{k^{\prime}}\right)$, since $p$ appears with multiplicity 1 in $\frac{d e}{k}$, but does not appear in $\frac{d^{\prime} e^{\prime}}{k^{\prime}}$. Therefore, the net contribution to the sum of all possible pairs $(u, v)$ given $m^{\prime}, n^{\prime}, d^{\prime}, e^{\prime}, k^{\prime}$ is $\mu\left(\frac{d^{\prime} e^{\prime}}{k^{\prime}}\right)$. In other words, adding one more distinct prime factor to $m, n, k$ does not change the value of the sum, or after trivial induction, the proposed result follows.

U276. Let $K$ be a finite field. Find all polynomials $f \in K[X]$ such that $f(X)=f(a X)$ for all $a \in K^{*}$.
Proposed by Mihai Piticari, Campulung Moldovenesc, Romania

Solution by Daniel Lasaosa, Universidad Pública de Navarra, Spain
It is well known that, if $K$ is a finite field, then there exists a prime $p$ such that the characteristic of $K$ is $p$, the order of $K$ is $p^{n}$ for some positive integer $n$, and this finite field is unique up to isomorphism. Moreover, the multiplicative group of this finite field (ie, the group with respect to multiplication of $K^{*}$ ), has order $p^{n}-1$ and $\varphi\left(p^{n}-1\right)$ primitive generators $g$, such that $K^{*}=\left\{g, g^{2}, \ldots, g^{p^{n}-1}=1\right\}$, where 1 denotes the unit of the multiplication operation.

Moreover, for all $a \in K^{*}$, we can take $X=1$, or $f(1)=f(a)$ for all $a \in K^{*}$. Therefore, any such polynomial takes a certain value $b$ for all $a \in K^{*}$, and a certain value (not necessarily distinct) $c$ for 0 (where 0 denotes the unit of the sum operation). Thus, any such polynomial $f$ can be written as $f(X)=d X^{p^{n}-1}+c$, where $c=f(0)$ and $d=b-c=f(1)-f(0)=f(a)-f(0)$ for all $a \in K^{*}$. Any other polynomial that satisfies the conditions given in the problem statement can be written equivalently in the proposed form.

## Olympiad problems

O271. Let $\left(a_{n}\right)_{n \geq 0}$ be the sequence given by $a_{0}=0, a_{1}=2$ and $a_{n+2}=6 a_{n+1}-a_{n}$ for $n \geq 0$. Let $f(n)$ be the highest power of 2 that divides $n$. Prove that $f\left(a_{n}\right)=f(2 n)$ for all $n \geq 0$.

Proposed by Albert Stadler, Herrliberg, Switzerland

Solution by G. C. Greubel, Newport News, VA
First consider the difference equation

$$
\begin{equation*}
a_{n+2}=6 a_{n+1}-a_{n} \tag{2}
\end{equation*}
$$

where $a_{0}=0$ and $a_{1}=2$. The solution of the difference equation can be obtained by making the approximation $a_{m}=r^{m}$ for which $r$ must satisfy the quadratic equation $r^{2}-6 r+1=0$. It is seen that $r=3 \pm 2 \sqrt{2}$ and leads to the general form

$$
\begin{equation*}
a_{n}=A(3+2 \sqrt{2})^{n}+B(3-2 \sqrt{2})^{n} . \tag{3}
\end{equation*}
$$

The values of $A$ and $B$ can be obtained from the initial values and leads to

$$
\begin{equation*}
a_{n}=\frac{1}{2 \sqrt{2}}\left[(3+2 \sqrt{2})^{n}-(3-2 \sqrt{2})^{n}\right] . \tag{4}
\end{equation*}
$$

Since $3+2 \sqrt{2}=(1+\sqrt{2})^{2}$ and $3-2 \sqrt{2}=(1-\sqrt{2})^{2}$ then $a_{n}$ becomes

$$
\begin{equation*}
a_{n}=\frac{(1+\sqrt{2})^{2 n}-(1-\sqrt{2})^{2 n}}{(1+\sqrt{2})-(1-\sqrt{2})} \tag{5}
\end{equation*}
$$

This last form can readily be seen as the Pell numbers of even values, namely, $a_{n}=P_{2 n}$.
The function $f(n)$ is the highest power of 2 that divides $n$. This works as follows: $f(0)=0, f(1)=0$, $f(2)=1, f(3)=0, f(4)=2, f(5)=0$, and so on. The function $f(n)$ is the set

$$
f(n) \in\{0,0,1,0,2,0,1,0,3,0,1,0,2,0,1,0,4,0,1,0,2, \cdots\}
$$

and is the sequence A007814 of the On-line Encyclopedia of Integers Sequences. The following table defines, for each $n$ value the corresponding $P_{2 n}, f(2 n)$ and $f\left(P_{2 n}\right)$ values.

| $n$ | $P_{2 n}$ | $f(2 n)$ | $f\left(P_{2 n}\right)$ |
| :---: | :---: | :---: | :---: |
| 0 | 0 | 0 | 0 |
| 1 | 2 | 1 | 1 |
| 2 | 12 | 2 | 2 |
| 3 | 70 | 1 | 1 |
| 4 | 408 | 3 | 3 |
| 5 | 2378 | 1 | 1 |
| 6 | 13860 | 2 | 2 |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |

Indeed it is seen that $f\left(P_{2 n}\right)=f(2 n)$ and thus the requirement of the problem is shown.
Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain; AN- anduud Problem Solving Group, Ulaanbaatar, Mongolia; Li Zhou, Polk State College, USA.

O272. Let $A B C$ be an acute triangle with orthocenter $H$ and let $X$ be a point in its plane. Let $X_{a}, X_{b}, X_{c}$ be the reflections of $X$ across $A H, B H, C H$, respectively. Prove that the circumcenters of triangles $A H X_{a}, B H X_{b}, C H X_{c}$ are collinear.

Proposed by Michal Rolinek, Institute of Science and Technology, Vienna and Josef Tkadlec, Charles University, Prague

Solution by Sebastiano Mosca, Pescara, Italy and Ercole Suppa, Teramo, Italy


Let $V_{a}, V_{b}, V_{c}$ be the circumcenters of triangles $A H X_{a}, B X H_{b}, C X H_{c}$ and let $W_{a}, W_{b}, W_{c}$ be the reflections of $V_{a}, V_{b}, V_{c}$ across $A H, B H, C H$, respectively; let $\ell_{a}, \ell_{b}, \ell_{c}$ be the perpendicular bisectors of $A H, B H, C H$ and denote $A_{1}=\ell_{b} \cap \ell_{c}, B_{1}=\ell_{a} \cap \ell_{c}, C_{1}=\ell_{a} \cap \ell_{b}$, as shown in figure.

Observe that the circles $\left(V_{a}\right) \equiv \odot\left(A H X_{a}\right),\left(V_{b}\right) \equiv \odot\left(B H X_{b}\right),\left(V_{c}\right) \equiv \odot\left(C H X_{c}\right)$ are respectively congruent to $\left(W_{a}\right) \equiv \odot(A H X),\left(W_{b}\right) \equiv \odot(B H X),\left(W_{c}\right) \equiv \odot(C H X)$.

The points $W_{a}, W_{b}, W_{c}$ belong to the perpendicular bisector of $H X$. Thus by applying the Menelaus' theorem to the triangle $A_{1}, B_{1}, C_{1}$ and to the transversal $W_{a} W_{b} W c$ we get

$$
\begin{equation*}
\frac{A_{1} W_{c}}{W_{c} B_{1}} \cdot \frac{B_{1} W_{a}}{W_{a} C_{1}} \cdot \frac{C_{1} W_{b}}{W_{b} A_{1}}=-1 \tag{1}
\end{equation*}
$$

Because of the symmetry clearly we have

$$
\begin{array}{llll}
A_{1} W_{c}=B_{1} V_{c} & , & B_{1} W_{a}=C_{1} V_{A} & ,
\end{array} \quad C_{1} W_{b}=A_{1} V_{b} ~ 子 ~ W_{c} B_{1}=V_{c} A_{1} \quad, \quad W_{a} C_{1}=V_{a} B_{1} \quad, \quad W_{b} A_{1}=V_{b} C_{1}
$$

From (1),(2),(3) it follows that

$$
\frac{A_{1} V_{b}}{V_{b} C_{1}} \cdot \frac{C_{1} V_{a}}{V_{a} B_{1}} \cdot \frac{B_{1} V_{c}}{V_{c} A_{1}}=\frac{A_{1} W_{c}}{W_{c} B_{1}} \cdot \frac{B_{1} W_{a}}{W_{a} C_{1}} \cdot \frac{C_{1} W_{b}}{W_{b} A_{1}}=-1
$$

so, by converse of Menelaus' theorem, the points $V_{a}, V_{b}, V_{c}$ are collinears, as required.
Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain; Georgios Batzolis, Mandoulides High School, Thessaloniki, Greece; Li Zhou, Polk State College, USA.

O273. Let $P$ be a polygon with perimeter $L$. For a point $X$, denote by $f(X)$ the sum of the distances to the vertices of $P$. Prove that for any point $X$ in the interior of $P, f(X)<\frac{n-1}{2} L$.

Proposed by Ivan Borsenco, Massachusetts Institute of Technology, USA

Solution by Daniel Lasaosa, Universidad Pública de Navarra, Spain
Claim: It suffices to show the proposed result for convex polygons.
Proof: If the polygon is concave, a sequence of consecutive vertices $V_{1}, V_{2}, \ldots, V_{k}$ with $k \geq 3$ exists such that line $V_{1} V_{k}$ leaves all the polygon on the same half-plane, and the region determined by $V_{1}, V_{2}, \ldots, V_{k}$ is outside the given polygon. Let $W_{2}, W_{3}, \ldots, W_{k-1}$ be the symmetric of $V_{2}, V_{3}, \ldots, V_{k-1}$ with respect to line $V_{1} V_{k}$. Note that for any point $X$ inside the original polygon, $X W_{i}>X V_{i}$ for $i=2,3, \ldots, k-1$, while the perimeter of the polygon resulting from deleting vertices $V_{2}, V_{3}, \ldots, V_{k-1}$ and substituting them by vertices $W_{2}, W_{3}, \ldots, W_{k-1}$ is the same as the perimeter of the original polygon. After a finite number of these transformations, we will obtain a convex polygon, and if the result is true for it, it will also be true for the original concave polygon. The Claim follows.

The proposed result is true for any triangle $A B C$ and any point $X$ inside it. Indeed, consider the ellipse with foci $B, C$ through $A$. This ellipse contains $X$ inside it, or $B X+C X<A B+C A$, and similarly for the result of cyclically permuting $A, B, C$. Adding all such inequalities and dividing by 2 we obtain

$$
f(X)=A X+B X+C X<A B+B C+C A=\frac{3-1}{2} L .
$$

Assume now that the result is true for any convex polygon with $n$ sides. Note that, when polygon $P$ has $n+1$ sides, there are always three consecutive vertices that we can denote $V_{n}, V_{n+1}, V_{1}$ such that $X$ is outside or on the perimeter of triangle $V_{n} V_{n+1} V_{1}$. Denote by $P^{\prime}$ the polygon $V_{1} V_{2} \ldots V_{n}$ (which clearly holds $X$ inside it or on its perimeter), by $f^{\prime}(X)$ the sum of distances from $X$ to the vertices of $P^{\prime}$, and by $L^{\prime}$ the perimeter of $V_{1} V_{2} \ldots V_{n}$. Then, $f(X)=f^{\prime}(X)+X V_{n+1}$, while by the triangle inequality, $L=$ $L^{\prime}+V_{n} V_{n+1}+V_{n+1} V_{1}-V_{n} V_{1}>L^{\prime}$. Now, by hypothesis of induction, $f^{\prime}(X)<\frac{n-1}{2} L^{\prime}<\frac{(n+1)-2}{2} L$, or it suffices to show that $X V_{n+1} \leq \frac{L}{2}$. Now, line $X V_{n+1}$ intersects the perimeter of $P$ at a second point $Y$, such that $X V_{n+1}<Y V_{n+1}$. When we move around the perimeter of $P$ from $Y$ to $V_{n+1}$, there is one direction in which the distance traveled is at most $\frac{L}{2}$, and by the triangle inequality $Y V_{n+1}<\frac{L}{2}$. The conclusion follows.

Also solved by Li Zhou, Polk State College, USA.

O274. Let $a, b, c$ be positive integers such that $a$ and $b$ are relatively prime. Find the number of lattice points in

$$
D=\{(x, y) \mid x, y \geq 0, b x+a y \leq a b c\} .
$$

Proposed by Arkady Alt, San Jose, California, USA

Solution by Li Zhou, Polk State College, USA
Let $X=(a c, 0)$ and $Y=(0, b c)$. Since the equation of $X Y$ is $y=b\left(c-\frac{x}{a}\right)$ and $a, b$ are relatively prime, $y$ is an integer if and only if $a \mid x$. Hence, the number of lattice points in the interior of segment $X Y$ is $c-1$. Then it is easy to see that the number of lattice points on the boundary of $D$ is $B=a c+b c+c$. Let $I$ be the the number of lattice points in the interior of $D$. By Pick's theorem, $I+\frac{1}{2} B-1$ equals the area of $D$, which is $\frac{1}{2} a b c^{2}$. Therefore, the number of lattice points in $D$ is

$$
I+B=\frac{1}{2}\left(a b c^{2}+B\right)+1=\frac{c(a b c+a+b+1)}{2}+1 .
$$

Also solved by Daniel Lasaosa, Universidad Pública de Navarra, Spain.

O275. Let $A B C$ be a triangle with circumcircle $\Gamma(O)$ and let $\ell$ be a line in the plane which intersects the lines $B C, C A, A B$ at $X, Y, Z$, respectively. Let $\ell_{A}, \ell_{B}, \ell_{C}$ be the reflections of $\ell$ across $B C, C A, A B$, respectively. Furthermore, let $M$ be the Miquel point of triangle $A B C$ with respect to line $\ell$.
a) Prove that lines $\ell_{A}, \ell_{B}, \ell_{C}$ determine a triangle whose incenter lies on the circumcircle of triangle $A B C$.
b) If $S$ is the incenter from (a) and $O_{a}, O_{b}, O_{c}$ denote the circumcenters of triangles $A Y Z, B Z X, C X Y$, respectively, prove that the circumcircles of triangles $S O O_{a}, S O O_{b}, S O O_{c}$ are concurrent at a second point, which lies on $\Gamma$.

Proposed by Cosmin Pohoata, Princeton University, USA

## Solution by Daniel Lasaosa, Universidad Pública de Navarra, Spain

a) Let $A^{\prime}=\ell_{B} \cap \ell_{C}, B^{\prime}=\ell_{C} \cap \ell_{A}$ and $C^{\prime}=\ell_{A} \cap \ell_{B}$. Note first that $Y$ is the point where $\ell, \ell_{B}, A C$ concur, or since $\ell, \ell_{B}$ are symmetric around $A C$, they are also symmetric around the perpendicular to $A C$ at $Y$, and we have $\angle Z Y A^{\prime}=180^{\circ}-2 \angle A Y Z$, and similarly $\angle Y Z A^{\prime}=180^{\circ}-2 \angle A Z Y$, hence

$$
\angle Y A^{\prime} Z=2(\angle A Y Z+\angle A Z Y)-180^{\circ}=180^{\circ}-2 \angle Y A Z=180^{\circ}-\angle Y O_{a} Z,
$$

hence $Y O_{a} Z A^{\prime}$ is cyclic. Moreover,

$$
\angle Y O_{a} A^{\prime}=\angle Y Z A^{\prime}=180^{\circ}-2 \angle A Z Y=180^{\circ}-\angle A O_{a} Y,
$$

hence $A, O_{a}, A^{\prime}$ are collinear. Finally, $\angle Y A^{\prime} A=\angle Y A^{\prime} O_{a}=\angle Y Z O_{a}$, and similarly $\angle Z A^{\prime} A=\angle Z Y O_{a}$, hence $A A^{\prime}$ is the angle bisector of $\angle Y A^{\prime} Z$, hence of $\angle B^{\prime} A^{\prime} C^{\prime}$. Or the incenter of $A^{\prime} B^{\prime} C^{\prime}$ is the point where $A O_{a}, B O_{b}, C O_{c}$ concur.

Let $S_{a}, S_{b}$ be the points where $A O_{a}, B O_{b}$ meet the circumcircle of $A B C$ for the second time. Clearly,

$$
\angle C A S_{a}=\angle Y A O_{a}=90^{\circ}-\frac{1}{2} \angle A O_{a} Y=90^{\circ}-\angle A Z Y
$$

and similarly $\angle C B S_{b}=90^{\circ}-\angle B Z X$. But $\angle A Z Y=\angle B Z X$ since it is the angle between $\ell$ and $A B$, or $S_{a}=S_{b}$. Similarly, $S_{b}=S_{c}$, or $A O_{a}, B O_{b}, C O_{c}$ meet at a point $S=S_{a}=S_{b}=S_{c}$ on the circumcircle of $A B C$, which is also the incenter of $A^{\prime} B^{\prime} C^{\prime}$. The conclusion to part a) follows.

Note: The previous argument breaks down when $A B C$ is obtuse because some of the angles cannot be added or subtracted as needed. Indeed, in this case, we can draw triangles $A B C$ for which the statement proposed in part a) is not true, and the incenter of $A^{\prime} B^{\prime} C^{\prime}$ may be inside triangle $A B C$ and not on its circumcircle.
b) It is well known that the Miquel point for $X \in B C, Y \in C A, Z \in A B$ such that $X, Y, Z$ are collinear, is on the circumcircle of $A B C$, hence $M$ is on the circumcircle of $A B C$. Assume wlog (since we may cyclically permute the vertices of $A B C$ without altering the problem) that $M$ is on the arc $A B$ that does not contain $C$. Since $M$ is on the circumcircle of $A Y Z$, the perpendicular bisector of $A M$ passes through $O, O_{a}$. At the same time, denoting by $T$ the point diametrally opposite $S$ in the circumcircle of $A B C$, we have, if for example $\angle S A M$ is acute and $\angle S B M$ is obtuse,

$$
\angle O S M=90^{\circ}-\angle S T M=90^{\circ}-\angle S A M=90^{\circ}-\angle O_{a} A M=\frac{1}{2} \angle A O_{a} M=180^{\circ}-\angle M O_{a} O
$$

and $M, O, O_{a}, S$ are concyclic, while at the same time

$$
\angle O S M=90^{\circ}-\angle S T M=\angle S B M-90^{\circ}=90^{\circ}-\angle O_{b} B M=\frac{1}{2} \angle B O_{b} M=\angle M O_{b} O,
$$

and again $M, O, O_{b}, S$ are concyclic. Similarly, since $\angle S C M$ is either acute or obtuse, we have one of these two cases, and $M, O, O_{c}, S$ are also concyclic. Hence the circumcircles of $S O O_{a}, S O O_{b}, S O O_{c}$ all meet again at $M$, which is a point on the circumcircle of $A B C$. The conclusion to part b) follows.

O276. For a prime $p$, let $S_{1}(p)=\left\{(a, b, c) \in \mathbf{Z}^{3}, \quad p \mid a^{2} b^{2}+b^{2} c^{2}+c^{2} a^{2}+1\right\}$ and $S_{2}(p)=\{(a, b, c) \in$ $\left.\mathbf{Z}^{3}, \quad p \mid a^{2} b^{2} c^{2}\left(a^{2}+b^{2}+c^{2}+a^{2} b^{2} c^{2}\right)\right\}$. Find all $p$ for which $S_{1}(p) \subset S_{2}(p)$.

Proposed by Titu Andreescu, University of Texas at Dallas and Gabriel Dospinescu, Ecole Polytechnique, Lyon, France

## Solution by the authors

The answer is $2,3,5,13$ and 17 . From now on we will work in $\mathbf{Z} / p \mathbf{Z}$ and consider $X_{1}(p)=\{(a, b, c) \in$ $\left.(\mathbf{Z} / p \mathbf{Z})^{3}, a^{2} b^{2}+b^{2} c^{2}+c^{2} a^{2}+1=0\right\}$ and $X_{2}(p)=\left\{(a, b, c) \in(\mathbf{Z} / p \mathbf{Z})^{3}, a^{2} b^{2} c^{2}\left(a^{2}+b^{2}+c^{2}+a^{2} b^{2} c^{2}\right)=0\right\}$. The condition $S_{1}(p) \subset S_{2}(p)$ is equivalent to $X_{1}(p) \subset X_{2}(p)$.

First, we prove that $2,3,5,13$ and 17 are solutions of the problem. Suppose that $p$ is one of these primes, that $(a, b, c) \in X_{1}(p)$ and that $(a, b, c) \notin X_{2}(p)$. In particular, $a^{2} b^{2} c^{2} \neq 0$. If one of $a^{2}, b^{2}, c^{2}$ equals 1 or -1 , then $a^{2} b^{2}+b^{2} c^{2}+c^{2} a^{2}+1$ and $a^{2}+b^{2}+c^{2}+a^{2} b^{2} c^{2}$ are equal or opposite, a contradiction. Hence $a^{2}, b^{2}, c^{2} \notin\{0, \pm 1\}$, which already settles the cases $p=2, p=3$ and $p=5$. If $p=13$, the squares $\bmod p$ are $0, \pm 1, \pm 3, \pm 4$, hence $a^{2}, b^{2}, c^{2} \in\{ \pm 3, \pm 4\}$ which means that two of them add up to 0 , say $a^{2}+b^{2}=0$. This readily yields $(a, b, c) \in X_{2}(p)$, a contradiction. Finally, suppose that $p=17$, so that the squares mod $p$ are $0, \pm 1, \pm 2, \pm 4, \pm 8$ and $a^{2}, b^{2}, c^{2} \in\{ \pm 2, \pm 4, \pm 8\}$. Moreover, no two of $a^{2}, b^{2}, c^{2}$ add up to 0 (same argument as before), and no two of them have product -1 . Hence up to permutation we have $\left(a^{2}, b^{2}, c^{2}\right) \in\{(2, \pm 4,-8),(-2, \pm 4,8)\}$, contradicting the fact that $(a, b, c) \in X_{1}(p)$.

Next, we prove that if $p>3$ is of the form $4 k+3$, then $X_{1}(p)$ is nonempty and disjoint from $X_{2}(p)$, hence $p$ is not a solution of the problem. Pick $c \in \mathbf{Z} / p \mathbf{Z}$ such that $c^{2} \notin\{0,1\}$ (such $c$ exists, since $p>3$ ). We will constantly use the fact that if $x, y \in \mathbf{Z} / p \mathbf{Z}$ satisfy $x^{2}+y^{2}=0$, then $x=y=0$. This implies that the map

$$
f:\left\{0,1, \ldots, \frac{p-1}{2}\right\} \rightarrow \mathbf{Z} / p \mathbf{Z}, \quad f(a)=-\frac{a^{2} c^{2}+1}{a^{2}+c^{2}}
$$

is well-defined and we claim that $f$ is injective. Indeed, if $f(a)=f\left(a_{1}\right)$, then an easy computation gives $\left(a^{2}-a_{1}^{2}\right)\left(c^{4}-1\right)=0$, hence $a=a_{1}$ (because $c^{2} \neq \pm 1$ ). Since $f$ is injective and since there are $\frac{p+1}{2}$ quadratic residues $\bmod p$, it follows that there are $a, b \in \mathbf{Z} / p \mathbf{Z}$ such that $f(a)=b^{2}$, which is equivalent to $(a, b, c) \in X_{1}(p)$. Hence $X_{1}(p) \neq \emptyset$. Suppose that $(a, b, c) \in X_{1}(p) \cap X_{2}(p)$. Since $p \equiv 3(\bmod 4)$, we have $a b c \neq 0$, hence $a^{2}\left(b^{2} c^{2}+1\right)+b^{2}+c^{2}=0$ and $a^{2}\left(b^{2}+c^{2}\right)+b^{2} c^{2}+1=0$. This yields $\left(a^{4}-1\right)\left(b^{2}+c^{2}\right)=0$, then $a^{2}=1$ and finally $\left(1+b^{2}\right)\left(1+c^{2}\right)=0$, a contradiction.

Suppose now that $p \equiv 1(\bmod 4)$ and $p>17$. We will construct an element of $X_{1}(p)$ which is not in $X_{2}(p)$, finishing the solution. Since $p \equiv 1(\bmod 4)$, there exists $x \in \mathbf{Z} / p \mathbf{Z}$ such that $x^{2}+1=0$. We will need the following

Lemma. The equation $a^{2}+a b+b^{2}=x$ has at least $p-1$ solutions $(a, b) \in \mathbf{Z} / p \mathbf{Z} \times \mathbf{Z} / p \mathbf{Z}$.
Proof. Write the equation as $(2 a+b)^{2}+3 b^{2}=4 x$. So it is enough to prove that the equation $u^{2}+3 v^{2}=t$ has at least $p-1$ solutions in $\mathbf{Z} / p \mathbf{Z} \times \mathbf{Z} / p \mathbf{Z}$, when $t \neq 0$. For each $v \in \mathbf{Z} / p \mathbf{Z}$, the equation $u^{2}=t-3 v^{2}$ has $1+\left(\frac{t-3 v^{2}}{p}\right)$ solutions, where $(\dot{\bar{p}})$ is Legendre's symbol. Hence the number of solutions $(u, v)$ is $p+\sum_{v \in \mathbf{Z} / p \mathbf{Z}}\left(\frac{t-3 v^{2}}{p}\right)$. It is not difficult to check that $\sum_{v \in \mathbf{Z} / p \mathbf{Z}}\left(\frac{t-3 v^{2}}{p}\right)$ equals $\pm 1$, according to whether -3 is a quadratic residue $\bmod p$ or not. This finishes the prof of the lemma.

Now let $S$ be the set of solutions of the previous equation. For each $(a, b) \in S$ we have an element $(a, b, c)$ of $X_{1}(p)$, where $c=-a-b$. Indeed,

$$
a^{2} b^{2}+b^{2} c^{2}+c^{2} a^{2}+1=(a b+b c+c a)^{2}+1=\left(a^{2}+a b+b^{2}\right)^{2}+1=x^{2}+1=0,
$$

hence $(a, b, c) \in X_{1}(p)$. Suppose that $(a, b, c) \in X_{2}(p)$. If $a=0$, then $b^{2}=x$ and $(a, b)$ takes at most two values. Similarly the cases $b=0$ and $c=0$ yield each at most 2 values for $(a, b)$, hence we have at most 6
solutions missed until now. Suppose that $a^{2}+b^{2}+c^{2}+a^{2} b^{2} c^{2}=0$. Since $a^{2}+b^{2}+c^{2}=2\left(a^{2}+b^{2}+a b\right)=2 x$ and $a^{2} c^{2}=(a(a+b))^{2}=\left(x-b^{2}\right)^{2}$, we obtain $2 x+b^{2}\left(x-b^{2}\right)^{2}=0$. This equation has at most 6 solutions in $\mathbf{Z} / p \mathbf{Z}$ and for each solution $b$ we loose at most two solutions $(a, b)$. Hence we loose at most 12 solutions of the equation $a^{2}+a b+b^{2}=x$ if $a^{2}+b^{2}+c^{2}+a^{2} b^{2} c^{2}=0$, and in total we loose at most 18 solutions. Since $p>17$ and $p \equiv 1(\bmod 4)$, we still have one solution $(a, b)$ and this yields an element of $X_{1}(p)$ which is not in $X_{2}(p)$.

