Solutions and Discussions

Problem 2 — Volume 28, No. 1, Spring 2004

Prove that $(p-1)!+1$ is divisible by p for each prime number p.

Solution

Raynold Gilles, Senior, Troy University, Troy, AL.

We must consider two cases

Case 1: $p = 2$

If $p = 2$, then $(p-1)!+1 = 2$, and clearly p divides $(p-1)!+1$.

Case 2: p is prime and different from 2.

We intend to show that $(p-1)! \equiv -1 \bmod p$, or equivalently, that $(p-1)!+1 \equiv 0 \bmod p$, from which it will follow that p divides $(p-1)!+1$.

To show that $(p-1)! \equiv -1 \bmod p$, we appeal to theorems involving cyclic groups. It is well known that if p is prime, then the set $\{1, 2, 3, \ldots, p-1\}$ forms a cyclic group under multiplication modulo n. The group is denoted $(\mathbf{Z}_p, \cdot)$. For example, $(\mathbf{Z}_5, \cdot)$ is a cyclic group generated by both 2 and 3. To see that 2 is a generator, note that $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, and $2^4 = 1$. Similarly, $3^1 = 3$, $3^2 = 4$, $3^3 = 2$, and $3^4 = 1$. For future reference, we make the observation that inherent in $(\mathbf{Z}_p, \cdot)$ being a group is the fact that it has no zero divisors.

Applying the theory of cyclic groups to our problem, we note that $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)$. Note that $(p-1)!$ is the product in which each element of the group $(\mathbf{Z}_p, \cdot)$ appears exactly once as a factor. Since $(\mathbf{Z}_p, \cdot)$ is cyclic, it has a generator g having

the property that:

$$\begin{array}{ccccl} g^{k_1} & = & 1 & & \text{for some } k_1 \in \{1,2,3,\ldots,p-1\} \\ g^{k_2} & = & 2 & & \text{for some } k_2 \in \{1,2,3,\ldots,p-1\} \\ g^{k_3} & = & 3 & & \text{for some } k_3 \in \{1,2,3,\ldots,p-1\} \\ \vdots & \vdots & \vdots & & \vdots \\ g^{k_{p-1}} & = & p-1 & & \text{for some } k_{p-1} \in \{1,2,3,\ldots,p-1\} \end{array}$$

Said differently:

$$\begin{array}{ccl} g^1 & = & \text{some element in } \{1,2,3,\ldots,p-1\} \\ g^2 & = & \text{some other element in } \{1,2,3,\ldots,p-1\} \\ \vdots & \vdots & \vdots \\ g^{p-1} & = & \text{the remaining element in } \{1,2,3,\ldots,p-1\}. \end{array}$$

$$\begin{aligned} \text{Thus, } (p-1)! \bmod p &\equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \bmod p \\ &= \left(g^1 \cdot g^2 \cdot g^3 \cdot \ldots \cdot g^{p-1}\right) \\ &= g^{1+2+3+\ldots+p-1} = g^{\frac{(p-1)p}{2}} = \left(g^{\frac{p-1}{2}}\right)^p \end{aligned}$$

i.e., $(p-1)! \bmod p = \left(g^{\frac{p-1}{2}}\right)^p$, where g is a generator of $(\mathbf{Z}_p, \cdot)$.

Since p is odd, the desired result, $(p-1)! \equiv -1 \bmod p$, will follow — provided that we can show that $g^{\frac{p-1}{2}} = -1$. Note that since g is a generator of $(\mathbf{Z}_p, \cdot)$, $g^{p-1} = 1$. (In fact, $p-1$ is the smallest positive power of g that yields 1.)

Since $g^{p-1} = 1$, it follows that:

$$\left(g^{\frac{p-1}{2}}\right)^2 = 1$$

$$\Rightarrow \left(g^{\frac{p-1}{2}}\right)^2 - 1 = 0$$

$$\Rightarrow \left(g^{\frac{p-1}{2}} + 1\right)\left(g^{\frac{p-1}{2}} - 1\right) = 0.$$

Since $(\mathbf{Z}_p, \cdot)$ has no zero divisors, we can conclude that either:

$g^{\frac{p-1}{2}} = -1$ or $g^{\frac{p-1}{2}} = 1$.

Since $p-1$ is the *least* positive power of g that yields 1, it follows that $g^{\frac{p-1}{2}} = -1$.

From this, the desired result follows.

One may wonder whether our proposition holds for all natural numbers p. (i.e., Is $(p-1)!+1$ is divisible by p for each natural number p?) The answer, as you might expect, is "no." As a counter-example, consider $p = 9$. We compute $(9-1)!+1 = 40321 = 4480 \cdot 9 + 1$. Clearly, $(p-1)!+1$ is not divisible by p for $p = 9$. Having established that counter-examples exist, we might wonder where the preceding proof "breaks down" in the case of a composite number such as $p = 9$. To answer this question, consider the set $\{1, 2, 3, \ldots, 8\}$ under the operation of multiplication modulo 9. We note that $3 \cdot 6 \equiv 0 \bmod 9$ (i.e. 3 and 6 are zero divisors.) Note also that the product $3 \cdot 6 = 0$ is *not* an element of the prospective group $(\mathbf{Z}_9, \cdot)$. Since $\{1, 2, 3, \ldots, 8\}$ is not closed under multiplication modulo 9, not only is $(\mathbf{Z}_9, \cdot)$ not a *cyclic* group, it is not a *group,* period. In reviewing the proof for the case in which p is prime, one will note that proof relied heavily on the facts that $(\mathbf{Z}_p, \cdot)$ is a cyclic group and that $(\mathbf{Z}_p, \cdot)$ has no zero divisors. It is at these places that the proof "breaks down."

Problem 7 — Volume 26, No. 2, Fall 2002

Given that $F(x) = \tan(x)$, prove that the n^{th} derivative $F^{(n)}(0) \geq 0$ for every $n \geq 0$.

Solution

William McCurdy, Senior, Troy University, Troy, AL.

We begin by proving a lemma.

Lemma 1: The derivative of any expression of the form $c\sec^m(x)\tan^n(x)$ with $c \geq 0$ and $m, n \geq 0$ is an expression comprised solely of terms of the form $c_i \sec^{m_i}(x)\tan^{n_i}(x)$ with $c_i \geq 0$ and $m_i, n_i \geq 0$.

PROOF. Using the product rule, note that: $\frac{d}{dx}\left[c\sec^m(x)\tan^n(x)\right] = cm\sec^m(x)\tan^{n+1}(x) + cn\tan^{n-1}(x)\sec^{m+2}(x)$ for $m, n \geq 0$.

i.e., $\frac{d}{dx}\left[c\sec^m(x)\tan^n(x)\right] = c_1\sec^{m_1}(x)\tan^{n_1}(x) + c_2\sec^{m_2}(x)\tan^{n_2}(x)$ with $c_1, c_2 \geq 0$ and $m_1, n_1, m_1, n_1 \geq 0$.

We now proceed to prove a second lemma, from which the desired result will follow.

Lemma 2: If $F(x) = \tan(x)$, then $F^{(n)}(x) = \sum_{i=1}^{2^{n-1}} c_i \sec^{m_i}(x)\tan^{n_i}(x)$ with $c_i \geq 0$ and $m_i, n_i \geq 0$.

PROOF. We prove the lemma by induction on n, the order of the derivative.

For $n = 0$, $F^{(n)}(x) = F^{(0)}(x) = \tan(x)$.

For the induction step, suppose that our proposition holds true for $n = k$. To compute $F^{(k+1)}(x)$, we compute $\frac{d}{dx}\left[F^{(k)}(x)\right] = \frac{d}{dx}\left[\sum_{i=1}^{2^{k-1}} c_i \sec^{m_i}(x)\tan^{n_i}(x)\right]$, by our induction hypothesis.

Since the derivative of a sum is computed "term by term," Lemma 1 tells us that upon differentiation, each term $c_i \sec^{m_i}(x)\tan^{n_i}(x)$ yields a pair of terms, $c_{i_1}\sec^{m_{i_1}}(x)\tan^{n_{i_1}}(x) + c_{i_2}\sec^{m_{i_2}}(x)\tan^{n_{i_2}}(x)$ with $c_{i_1}, c_{i_2} \geq 0$ and $m_{i_1}, n_{i_1}, m_{i_2}, n_{i_2} \geq 0$. Renumbering the subscripts, we have:

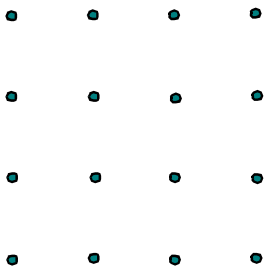
$$F^{(k+1)}(x) = \frac{d}{dx}\left[F^{(k)}(x)\right] = \sum_{i=1}^{2^k} c_i \sec^{m_i}(x)\tan^{n_i}(x).$$

Thus, $F^{(n)}(x) = \sum_{i=1}^{2^{n-1}} c_i \sec^{m_i}(x)\tan^{n_i}(x)$ with $c_i \geq 0$ and $m_i, n_i \geq 0$.

Since $\sec^{m_i}(0) = 1$ and $\tan^{n_i}(0) = 0$, each term of $F^{(n)}(0) = \sum_{i=1}^{2^{n-1}} c_i \sec^{m_i}(0)\tan^{n_i}(0)$ is non-negative. Hence, $F^{(n)}(0) \geq 0$ for every $n \geq 0$.

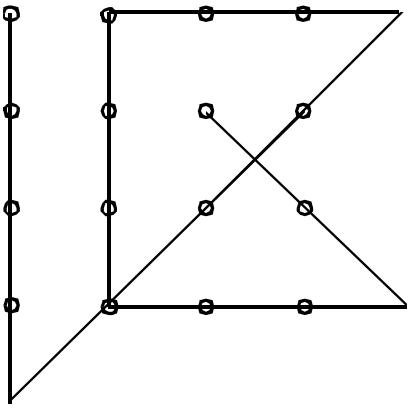
Problem 7 — Volume 29, No. 1&2, Spring/Fall 2005

Draw six line segments through these 16 points, which are arranged in a grid. Do not lift your pencil from start to finish.



Solution

Jenny Horton, Senior, Troy University, Troy, AL.



Having seen a solution, one might wonder if it is possible to solve the problem using *fewer* than six line segments. Since the 16 points are arranged in a 4×4 grid, no line segment (vertical, horizontal, or diagonal) can contain more than 4 points. So clearly, the task cannot be completed with fewer than four line segments.

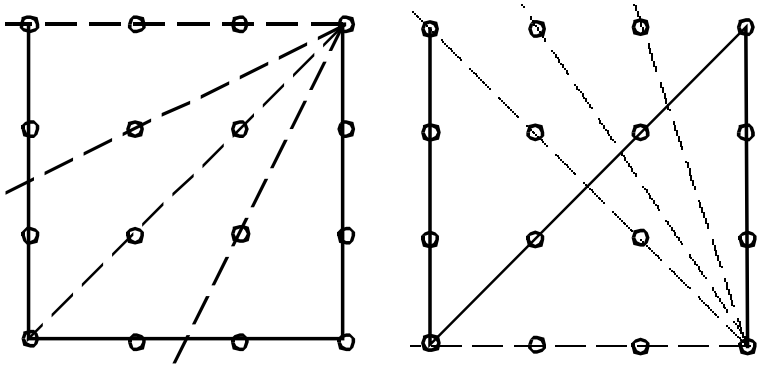
Case 1: 4 Segments

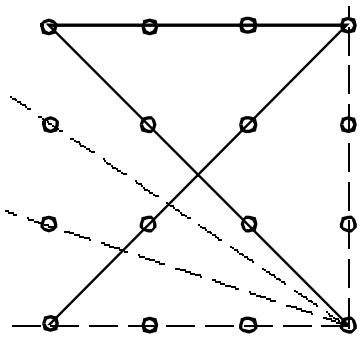
Since no line segment can contain more than four points, each line segment must contain exactly four points, and in each case, none of these four points must be contained by any other line segment. The line segments cannot all be vertical, since these cannot be drawn without having the pencil leave the paper. Similarly, the line segments cannot all be horizontal. The lines cannot all be diagonal, as only two diagonal lines contain 4 points. No combination of diagonals and horizontals will work as a diagonal containing 4 points will contain a point from each row. Thus, if one of the line segments is diagonal, no horizontal line segment can contain 4 points in such a way that none of the 4 points are contained in and "claimed" by another line segment. Similarly, no vertical/diagonal, vertical/horizontal, or vertical/horizontal/diagonal combination of line segments will work.

Case 2: 5 Segments

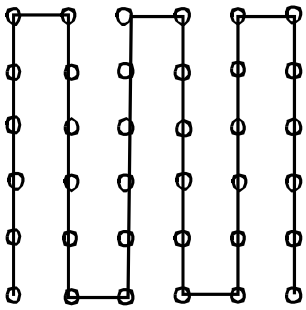
By the Pigeon Hole Principle, at least one line segment must contain at least four points (hence *exactly* four points) that are not accounted for on any other line segment. By reasons stated in the previous case, no other line segment can contain 4 points, This implies that the remaining 4 line segments must each contain *exactly* 3 points that are not accounted for on any of the other line segments. Thus, any three successive line segments can contain, at most, $4 + 3 + 3 = 10$ distinct points. Note from the diagrams

below, that any combination of vertical, horizontal and diagonal line segments containing 10 distinct points is such that the next line segment drawn must contain only 2 points not accounted for on other line segments. Thus, our problem cannot be solved using 5 line segments.



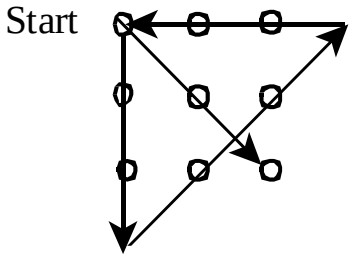


One may wonder what kind of bounds can be placed on the number of line segments required to solve the problem for an arbirary $n \times n$ grid for $n \geq 3$. From the diagram below, we can easily see that no more than $2n - 1$ line segments (e.g., n vertical and and $n - 1$ horizontal) are required in order to pass through all n^2 points.

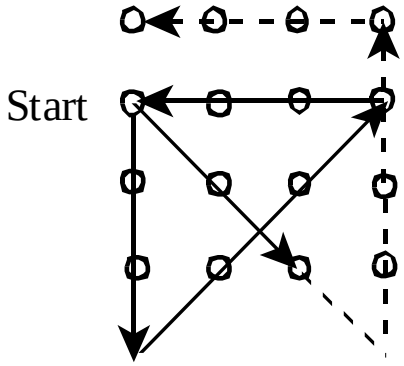


Having established an upper bound on the least number of line segments required, we claim that for an $n \times n$ grid with $n \geq 3$, no more than $2n - 2$ line segments are required. Furthermore, we claim that for an $n \times n$ grid with $n \geq 3$, all points of the grid can always be covered by $2n - 2$ line segments. We prove the claim by induction on n.

Observe, from the picture below, that in the $3 \asymp 3$ case, all points of the grid can be covered by $2n - 2 = 4$ line segments. Furthermore, for reasons similar to those given in the $4 \asymp 4$ case, no three sucessive line segments (drawn without lifting the pencil from the paper) can contain more than $3 + 2 + 2 = 7$ points. Thus, our proposition is true for $n = 3$.



Note further, that the diagram for $n = 3$ can be embedded in a 4×4 grid in such a way that by extending the last line segment diagonally downward, adding a line segment going upward, and following up with a line segment going to the left (see below), we have a diagram in which all 16 points of the 4×4 grid can be contained by $2n - 2 = 6$ line segments. Furthermore, we have already shown that the points of a 4×4 grid cannot be covered by fewer than $2n - 2 = 6$ line segments.

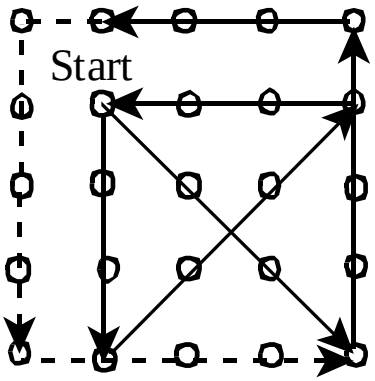


For the induction step, note that if our proposition is true for $n = k \geq 4$, then our diagram can be embedded in an $(k+1) \times (k+1)$ grid in such a way that:

(1) the last line segment of the diagram for $n = k$ can be extended horizontally or vertically by one unit and

(2) two more line segments of length $k+1$ and k can be drawn to form a diagram in which all $(k+1)^2$ points are contained by the line segments. Since the diagram for the $k \times k$ grid had $2k-2$ line segments, the diagram for the $(k+1) \times (k+1)$ grid has $(2k-2)+2 = 2(k+1)-2$ line segments.

The extension of a diagram for $k = 4$ to a diagram for $k+1 = 5$ is shown below.



It remains to show that our $(k+1) \times (k+1)$ grid can't be covered by fewer than $2(k+1)-2$ line segments. Generalizing an observation made in the 4×4 case, any three successive line

segments can contain, at most, $(k+1)+k+k$ distinct points, and any two successive line segments can contain, at most, $(k+1)+k$ distinct points. We will quickly note that the last two line segments that were added to the $k \times k$ diagram to extend it to a $(k+1) \times (k+1)$ diagram contain $(k+1)+k$ distinct points. No two line segments in a $(k+1) \times (k+1)$ grid can contain more points. So if we're looking to reduce the total number of line segments, we must consider the "original" $k \times k$ diagram that was embedded in the $(k+1) \times (k+1)$ grid. By our induction hypothesis, the $k \times k$ diagram is covered by $2k-2$ line segments, and this is the least number of line segments that can cover the $k \times k$ grid. So if we were to remove one of the line segments covering the "original" $k \times k$ grid, the resulting uncovered points would have to be covered by the last two line segments that were added to the "original" $k \times k$ diagram to extend it to a $(k+1) \times (k+1)$ diagram. But these two line segments already contain as many points as two line segments in a $(k+1) \times (k+1)$ grid can possibly contain, and hence cannot be used to cover any points from the "original" $k \times k$ diagram.

Solutions, comments, and discussions should be sent to:

Hussain Talibi
Department of Mathematics
Tuskegee University
Tuskegee, AL 36088
(334)-727-8212
talibi@tuskegee.edu

Pat Rossi
Department of Math & Physics
232 MSCX
Troy State University
Troy, AL 36082
(334)670-3406
FAX (334)670-3796
prossi@troyst.edu

ACTM Fall Forum 2009

Exploring Math from Many Angles

October 15-16

Auburn University Montgomery

Thursday, October 15 - Starting at 1 pm (Registration Begins at 12)

For more information go to http://www.alabamamath.org

Speaker proposal forms are also available at the address above.