MathemAttic

No. 3

The problems featured in this section are intended for students at the secondary school level.

Click here to submit solutions, comments and generalizations to any problem in this section.

To facilitate their consideration, solutions should be received by **June 15, 2019**.

MA11. Let $f(x) = 375x^5 - 131x^4 + 15x^2 - 435x - 2$. Find the remainder when $f(97)$ is divided by 11.

MA12. Ten straight lines are drawn on a two-dimensional plane. Given that three of these lines are parallel to one another, what is the maximum possible number of intersection points formed by the lines?

MA13. How many ways can the letters of the word LETTERKENNY be arranged in a row if the R must stay in the middle position and the letters L,R,K and Y must remain in their current order LRKY? (An example of an arrangement that meets the requirements is ELTTERENKYN.)

MA14. In $\triangle ABC$, the side AB has length 20 and $\angle ABC = 90°$. If the lengths of the other sides must be positive integers, how many such triangles are possible?

MA15. Prove that $43^{43} - 17^{17}$ is divisible by 10. (Do not use Fermat's Little Theorem.)

Les problèmes proposés dans cette section sont appropriés aux étudiants de l'école secondaire.

Cliquez ici afin de soumettre vos solutions, commentaires ou généralisations aux problèmes proposés dans cette section.

Pour faciliter l'examen des solutions, nous demandons aux lecteurs de les faire parvenir au plus tard le **15 juin 2019**.

La rédaction souhaite remercier Rolland Gaudet, professeur titulaire à la retraite à l'Université de Saint-Boniface, d'avoir traduit les problèmes.

MA11. Soit $f(x) = 375x^5 - 131x^4 + 15x^2 - 435x - 2$. Déterminer le reste lorsqu'on divise $f(97)$ par 11.

MA12. Dix lignes droites sont tracées dans le plan. Sachant que trois de ces lignes sont parallèles les unes aux autres, déterminer le nombre maximum de points d'intersection de ces lignes.

MA13. De combien de manières les chiffres présents dans le nombre 15665235774 peuvent-ils être permutés de façon à ce que le chiffre 2 reste au centre et que les chiffres 1, 2, 3 et 4 restent dans l'ordre initial 1234 ? (Un exemple d'un réarrangement respectant ces contraintes serait 51665257347.)

MA14. Le côté AB du $\triangle ABC$ est de longueur 20; aussi, $\angle ABC = 90°$. Si les longueurs des deux autres côtés doivent être des entiers positifs, déterminer le nombre de triangles possibles.

MA15. Sans utiliser le petit théorème de Fermat, démontrer que $43^{43} - 17^{17}$ est divisible par 10.

CONTEST CORNER SOLUTIONS

Statements of the problems in this section originally appear in 2018: 44(5), p. 185–186; and 44(6), p. 234–236.

CC321. Six boxes are numbered $1, 2, 3, 4, 5$ and 6. Suppose that there are N balls distributed among these six boxes. Find the least N for which it is guaranteed that for at least one k, box number k contains at least k^2 balls.

Originally Problem 4 from the 2015 Purple Comet! Math Meet.

We received 8 solutions. We present the solution by Ivko Dimitrić, slightly edited.

The least value of N is one more than the largest number M of balls that can be arranged so that for each k, the box number k contains less than k^2 balls. Since the largest value of such number M is sought, the k-th box should contain $k^2 - 1$ balls, thus

$$M = \sum_{k=1}^{6} (k^2 - 1) = 0 + 3 + 8 + 15 + 24 + 35 = 85.$$

Therefore, $N = 86$ is the smallest number that will guarantee that box number k contains at least k^2 balls for at least one value of k.

CC322. Suppose that the vertices of a polygon all lie on a rectangular lattice of points where adjacent points on the lattice are at distance 1 apart. Then the area of the polygon can be found using Pick's Formula: $I + \frac{B}{2} - 1$, where I is the number of lattice points inside the polygon, and B is the number of lattice points on the boundary of the polygon. Pat applied Pick's Formula to find the area of a polygon but mistakenly interchanged the values of I and B. As a result, Pat's calculation of the area was too small by 35. Using the correct values for I and B, the ratio $n = \frac{I}{B}$ is an integer. Find the greatest possible value of n. (*Ed.:* For more information on Pick's formula, take a look at the article *Two Famous Formulas (Part I)*, ***Crux*** 43 (2), p. 61–66.)

Originally Problem 11 from the 2015 Purple Comet! Math Meet.

We received 5 submissions of which 4 were correct and complete. We present the solution by Ivko Dimitrić.

The stated condition gives

$$I + \frac{B}{2} - 1 = B + \frac{I}{2} - 1 + 35,$$

which simplifies to $I - B = 70$. Then $n = \dfrac{I}{B} = \dfrac{70}{B} + 1$ is an integer, so $\dfrac{70}{B}$ must

also be an integer, i. e. B is a positive integer divisor of $70 = 2 \cdot 5 \cdot 7$ and since $B \geq 3$ (a lattice polygon has at least 3 vertices) we have $B \in \{5, 7, 10, 14, 35, 70\}$.

The largest value of n is obtained for the smallest possible value of B. When $B = 5$, then $n = \frac{70}{5} + 1 = 15$, implying $I = nB = 75$, and indeed there is a polygon (quadrilateral) that has exactly $B = 5$ lattice points on the boundary and $I = 75$ points in the interior. Such a polygon can be constructed as follows. Choose an arbitrary lattice point as the origin $(0, 0)$ of a rectangular coordinate system with perpendicular x- and y-axis running along adjacent sides of a unit square cell of the lattice, each containing an infinite sequence of lattice points that are 1 unit apart. The quadrilateral with vertices $(0, -1)$, $(0, 1)$, $(1, 1)$ and $(76, 0)$ contains five points on the boundary (the four vertices and the origin) and 75 points $(k, 0)$, $k = 1, 2, \ldots, 75$ along the x-axis in the interior, which are the only points of the lattice inside the polygon. Namely, the side joining vertices $(0, -1)$ and $(76, 0)$ with positive slope makes it impossible for any lattice point below the x-axis to belong to the interior or lie on that side, other than the vertex $(0, -1)$, and the side joining $(1, 1)$ and $(76, 0)$ with negative slope makes it impossible for any lattice point above the x-axis to be in the interior or lie on that side, other than the vertex $(1, 1)$. Thus, all the interior points are those 75 points on the x-axis and the only boundary lattice points are the five mentioned. For such a polygon, the maximum value $n = 15$ is attained.

CC323. Evaluate

$$\frac{\log_{10}(20^2) \cdot \log_{20}(30^2) \cdot \log_{30}(40^2) \cdots \log_{990}(1000^2)}{\log_{10}(11^2) \cdot \log_{11}(12^2) \cdot \log_{12}(13^2) \cdots \log_{99}(100^2)}$$

Originally Problem 14 from the 2015 Purple Comet! Math Meet.

We received 13 submissions of which 11 were correct and complete. We present the solution by Tyler McGilvry-James.

Expand the given expression by the logarithmic power rule:

$$\begin{aligned}
&\frac{\log_{10}(20^2) \cdot \log_{20}(30^2) \cdot \log_{30}(40^2) \cdots \log_{990}(1000^2)}{\log_{10}(11^2) \cdot \log_{11}(12^2) \cdot \log_{12}(13^2) \cdots \log_{99}(100^2)} \\
&\quad = \frac{2^{99} \log_{10}(20) \cdot \log_{20}(30) \cdot \log_{30}(40) \cdots \log_{990}(1000)}{2^{90} \log_{10}(11) \cdot \log_{11}(12) \cdot \log_{12}(13) \cdots \log_{99}(100)} \\
&\quad = 2^9 \frac{\log_{10}(20) \cdot \log_{20}(30) \cdot \log_{30}(40) \cdots \log_{990}(1000)}{\log_{10}(11) \cdot \log_{11}(12) \cdot \log_{12}(13) \cdots \log_{99}(100)}.
\end{aligned}$$

Consider the two quotients. We use the change of base formula:

$$\begin{aligned}
&\log_{10}(20) \cdot \log_{20}(30) \cdot \log_{30}(40) \cdots \log_{990}(1000) \\
&\quad = \frac{\log 20}{\log 10} \frac{\log 30}{\log 20} \cdots \frac{\log 990}{\log 980} \frac{\log 1000}{\log 990} = \frac{\log 1000}{\log 10} = 3
\end{aligned}$$

and

$$\log_{10}(11)\cdot\log_{11}(12)\cdot\log_{12}(13)\cdots\log_{99}(100)$$
$$=\frac{\log 11}{\log 10}\frac{\log 12}{\log 11}\cdots\frac{\log 99}{\log 98}\frac{\log 100}{\log 99}=\frac{\log 100}{\log 10}=2.$$

Thus the original expression can be simplified to $\frac{(3)(2^9)}{2}=768$. So we see that

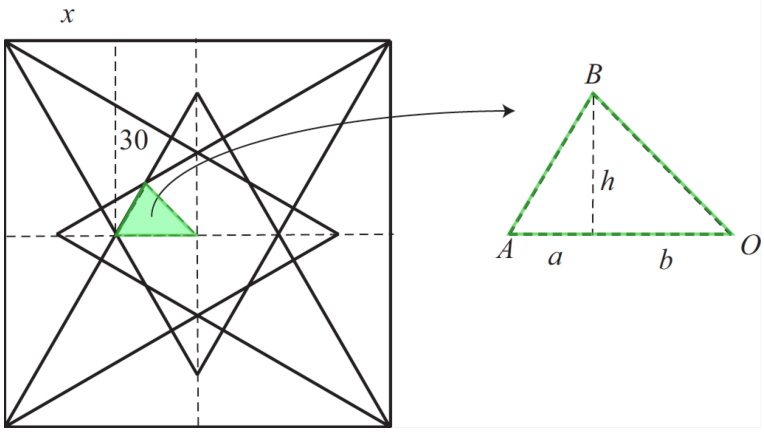
$$\frac{\log_{10}(20^2)\cdot\log_{20}(30^2)\cdot\log_{30}(40^2)\cdots\log_{990}(1000^2)}{\log_{10}(11^2)\cdot\log_{11}(12^2)\cdot\log_{12}(13^2)\cdot\log_{99}(100^2)}=768.$$

CC324. On the inside of a square with side length 60, construct four congruent isosceles triangles each with base 60 and height 50, and each having one side coinciding with a different side of the square. Find the area of the octagonal region common to the interiors of all four triangles.

Originally Problem 15 from the 2015 Purple Comet! Math Meet.

We received 5 submissions of which four were correct and complete. We present the solution by Ángel Plaza, modified by the editor.

Below we depict the said square and four congruent isosceles triangles while constructing the triangle ABO.



The area of the octagonal region common to the interiors of all triangles is eight times the area of the triangle ABO. By the property of similar triangles $\frac{30}{x}=\frac{50}{30}$, thus $x=18$. It follows that $|AO|=\frac{60}{2}-x=12$.

Let us consider $|AO|=a+b$, where a and b are respectively the projections of sides AB and BO over AO. Define C as the point of $h\perp AO$. By symmetry $\angle COB=\frac{\pi}{4}$. This implies that $\angle COB$ is an isosceles triangle, thus $h=b$. By the

property of similar triangles, we have $\frac{h}{a} = \frac{50}{30}$, which implies $a = \frac{3h}{5}$. We observe that

$$12 = a + b = \frac{3h}{5} + h \Rightarrow h = 7.5.$$

Therefore Area$(ABO) = \frac{12 \cdot 7.5}{2} = 45$. In conclusion, the area of the octagonal region is $8 \cdot 45 = 360$.

CC325. Seven people of seven different ages are attending a meeting. The seven people leave the meeting one at a time in random order. Given that the youngest person leaves the meeting sometime before the oldest person leaves the meeting, the probability that the third, fourth, and fifth people to leave the meeting do so in order of their ages (youngest to oldest) is $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

Originally Problem 26 from the 2015 Purple Comet! Math Meet.

We received 3 submissions of which 1 was correct and complete. We present the solution by Ivko Dimitrić.

Let $\{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$ be the set of persons, appearing in order in which they left the meeting, so p_i was the ith person who left the meeting on a time-line. Let $S = \{p_3, p_4, p_5\}$ be the subset composed of persons who left third, fourth and fifth and let y and o denote the youngest and the oldest person, respectively. Either y or o or both could belong to S and it is also possible that S contains neither y nor o. Let A denote the event that the third, fourth, and fifth persons left the meeting in age-increasing order and let B denote the event that y leaves the meeting before o does. Then we are asked to find the conditional probability

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

The number of favorable outcomes for B is $\binom{7}{2} \cdot 5! = 21 \cdot 5!$, since (y, o) couple can be chosen in $\binom{7}{2}$ ways among 7 time slots (numbered 1 through 7) for conference leaving and the remaining 5 time slots can be taken arbitrarily by the remaining 5 people in 5! ways, for which the age order is irrelevant. To determine the number of favourable outcomes for $A \cap B$ we do the counting depending on whether y and o belong to S.

(1) If $y \in S$ and $o \in S$, then necessarily $p_3 = y$ and $p_5 = o$, since p_3, p_4, p_5 would have to conform to age-ordering where p_4 is older than p_3 but younger than p_5. With $p_3 = y$, $p_5 = o$ fixed, the remaining five people can take arbitrarily five remaining time slots in 5! ways, since whoever happens to be p_4 will be of age between those of p_3 and p_5.

(2) If $y \in S$ but $o \notin S$, then $p_3 = y$ per force, since otherwise person p_3 would be older than $y \in \{p_4, p_5\}$, violating age ordering within S. Then $o \in \{p_6, p_7\}$ (2 possibilities) and the positions p_4, p_5 are occupied by an age-ordered pair among

the remaining 5 people in $\binom{5}{2}$ ways, whereas the remaining 3 slots can be taken by the remaining 3 people in 3! ways without regard to their ages. This makes for $\binom{5}{2} \cdot 2 \cdot 3! = 5!$ ways.

(3) If $y \notin S$ and $o \in S$, this case is dual to the previous one, where now $p_5 = o$ and there are two possibilities for $y \in \{p_1, p_2\}$. The places for p_3, p_4 can be taken by any age-ordered couple of people in $\binom{5}{2}$ ways and remaining three time-slots are taken by the remaining three people in 3! ways. This accounts again for $\binom{5}{2} \cdot 2 \cdot 3! = 5!$ favorable outcomes.

(4) If $y \notin S$ and $o \notin S$, then there are $\binom{4}{2} = 6$ ways of arranging y and o among p_1, p_2, p_6 and p_7. The places p_3, p_4, p_5 can be taken by any age-ordered triple among the remaining 5 people in $\binom{5}{3}$ ways, whereas the two remaining slots can be then taken arbitrarily in 2! ways by the remaining two people. So in this case we have $6 \cdot \binom{5}{3} \cdot 2! = 5!$ ways as well. Thus, the number of favourable outcomes for $A \cap B$ is $4 \cdot 5!$ and the required conditional probability is

$$P(A|B) = \frac{4 \cdot 5!/7!}{21 \cdot 5!/7!} = \frac{4}{21} = \frac{m}{n},$$

so that $m + n = 25$.

CC326. For positive integer n, let a_n be the integer consisting of n digits of 9 followed by the digits 488. For example, $a_3 = 999488$ and $a_7 = 9999999488$. For each given n, determine the largest integer $f(n)$ such that $2^{f(n)}$ divides a_n.

Originally Problem 19 from the Middle School 2013 Purple Comet! Math Meet.

We received eight submissions of which seven were correct and complete. We present the solution of Ivko Dimitric, modified by the editor.

The difference between a_n and the nearest power of ten, 10^{n+3}, is $512 = 2^9$. Algebraically,

$$a_n = 10^{n+3} - 2^9 = 2^{n+3}5^{n+3} - 2^9.$$

We consider the following three cases:

(i) For $1 \leq n < 6$, we have that

$$a_n = 2^{n+3}(5^{n+3} - 2^{6-n}),$$

with the number in the parentheses being odd. Thus, $f(n) = n + 3$.

(ii) If $6 < n$, then

$$a_n = 2^9(2^{n-6}5^{n+3} - 1),$$

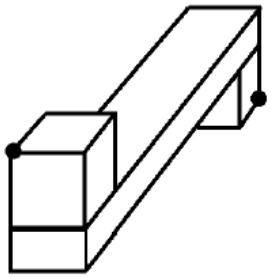
with the number in parentheses being odd. Thus we have that $f(n) = 9$.

(*iii*) If $n = 6$, then by the binomial expansion theorem

$$\begin{aligned} a_n &= 2^9(5^9 - 1) \\ &= 2^9[(4+1)^9 - 1] \\ &= 2^9\left[4^9 + 9 \cdot 4^8 + \binom{9}{2}4^7 + \cdots + \binom{9}{7}4^2 + 9 \cdot 4\right] \\ &= 2^{11}\left[4^8 + 9 \cdot 4^7 + \binom{9}{2}4^6 + \cdots + \binom{9}{7}4 + 9\right]. \end{aligned}$$

The number inside the brackets is odd. Thus we have that $f(6) = 11$.

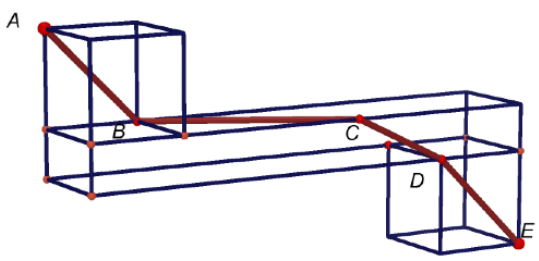
CC327. The diagram below shows a $1 \times 2 \times 10$ duct with $2 \times 2 \times 2$ cubes attached to each end. The resulting object is empty, but the entire surface is solid sheet metal. A spider walks along the inside of the duct between the two marked corners. There are positive integers m and n so that the shortest path the spider could take has length $\sqrt{m} + \sqrt{n}$. Find $m + n$.



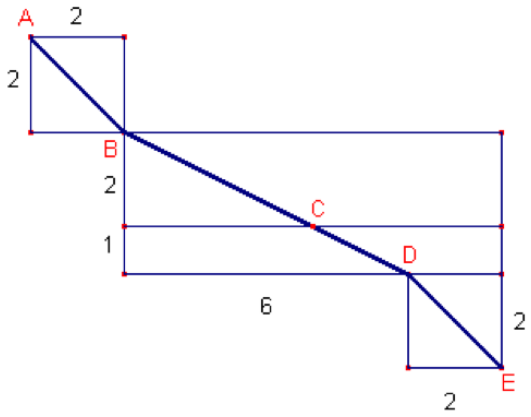
Originally Problem 20 from the 2013 Purple Comet! Math Meet.

We received one submission which was correct and complete. We present the solution of Ricard Peiró.

The shortest path is formed by the polygonal line $ABCDE$, shown in the below figure:



Laid flat, the path is as follows:



The lengths of segments of the path AB, BD, and DE are $2\sqrt{2}$, $3\sqrt{5}$, and $2\sqrt{2}$, respectively. The total length of said path is

$$AB + BD + DE = 4\sqrt{2} + 3\sqrt{5} = \sqrt{32} + \sqrt{45}.$$

Thus $m = 32$, $n = 45$, and $m + n = 77$.

CC328. You have many identical cube-shaped wooden blocks. You have four colours of paint to use, and you paint each face of each block a solid colour so that each block has at least one face painted with each of the four colours. Find the number of distinguishable ways you could paint the blocks. (Two blocks are distinguishable if you cannot rotate one block so that it looks identical to the other block.)

Originally Problem 18 from the 2015 Purple Comet! Math Meet.

We received one solution by C.R. Pranesachar, which we present below in slightly edited form.

We use Pólya's enumeration theorem. For the group of 24 rotations of the cube, the cycle index (for faces) is given by

$$Z(t_1, t_2, t_3, t_4) = \frac{1}{24}(t_1^6 + 6t_1^2t_4 + 3t_1^2t_2^2 + 8t_3^2 + 6t_2^3).$$

Let x, y, z, w be the variables for the number of faces of the cube that are painted with the four colours. We let $\sum x^k$ denote $x^k + y^k + z^k + w^k$ for $1 \le k \le 4$. Then the colour-counting polynomial is given by

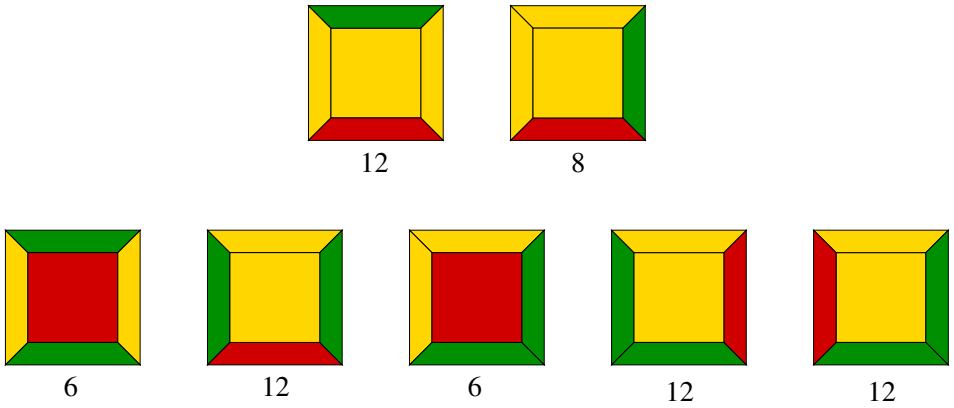
$$\begin{aligned} g(x, y, z, w) &= Z(\textstyle\sum x, \sum x^2, \sum x^3, \sum x^4) \\ &= \frac{1}{24}(\textstyle\sum x)^6 + 6(\sum x)^2(\sum x^4) + 3(\sum x)^2(\sum x^2)^2 + 8(\sum x^3)^2 + 6(\sum x^2)^3. \end{aligned}$$

Since all the four colours are to be used, we need the sum of the coefficients of the terms containing all of x, y, z, w in $g(x, y, z, w)$. This occurs only in $(\sum x)^6$ and $3(\sum x)^2(\sum x^2)^2$. Accordingly the sum of the coefficients is equal to

$$\frac{1}{24}\left(\frac{6!}{3!1!1!1!}\cdot 4+\frac{6!}{2!2!1!1!}\cdot 6+3\cdot 2\cdot 2\cdot 6\right)=\frac{1}{24}(480+1080+72)=68,$$

which is the desired answer.

Editor's comment. The possible colourings of the cube can be seen in the figure. The invisible face is coloured with the fourth colour. The number under each configuration indicates how many distinct cubes are obtained by permuting the four colours of each configuration.



CC329. Let a, b, c and d be real numbers such that

$$a^2+3b^2+\frac{c^2+3d^2}{2}=a+b+c+d-1.$$

Find $1000a+100b+10c+d$.

Originally Problem 19 from the 2015 Purple Comet! Math Meet.

We received 8 correct solutions. We present the solution by Sěfket Arslanagić.

We have

$$\begin{aligned}
&a^2+3b^2+\frac{c^2+3d^2}{2}=a+b+c+d-1 \iff\\
&a^2+3b^2+\frac{1}{2}c^2+\frac{3}{2}d^2-a-b-c-d+1=0 \iff\\
&\left(a-\frac{1}{2}\right)^2+3\left(b-\frac{1}{6}\right)^2+\frac{1}{2}(c-1)^2+\frac{3}{2}\left(d-\frac{1}{3}\right)^2=0.
\end{aligned}$$

From here, we conclude that $a=\frac{1}{2}, b=\frac{1}{6}, c=1$ and $d=\frac{1}{3}$. It follows that

$$1000a+100b+10c+d=500+\frac{50}{3}+10+\frac{1}{3}=510+17=527.$$

CC330. Six children stand in a line outside their classroom. When they enter the classroom, they sit in a circle in random order. There are relatively prime positive integers m and n so that $\frac{m}{n}$ is the probability that no two children who stood next to each other in the line end up sitting next to each other in the circle. Find $m+n$.

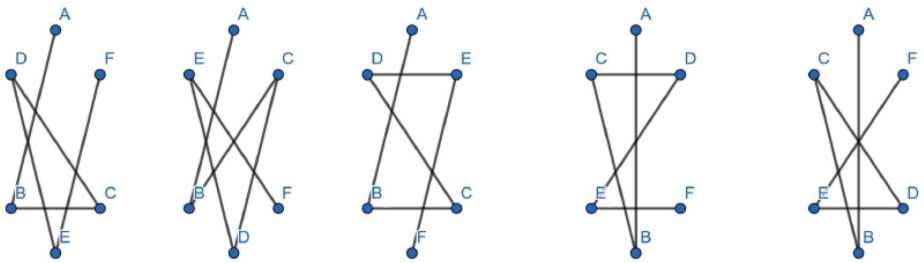
Originally Problem 18 from the Middle School 2013 Purple Comet! Math Meet.

We received 2 correct solutions. Solution by C. R. Pranesachar.

Let the children standing in a line be named A, B, C, D, E, F, in that order, while standing outside the classroom. When they are seated around a circle, in order to satisfy the given non-adjacency condition, we need to take hamiltonian paths along the diagonals of the hexagon and go through all of the vertices, naming them from A to F respectively. We get the 5 diagrams below and their reflections in the vertical line through A. Thus there are $5 \times 2 = 10$ paths only. Since rotation does not change adjacency, we infer that the probability according to the given condition is

$$\frac{10 \times 6}{6!} = \frac{60}{720} = \frac{1}{12}.$$

Thus $m = 1$ and $n = 12$, giving $m + n = 13$.



PROBLEM SOLVING VIGNETTES

No.3

Donald Rideout

Arithmetic of Remainders

Divisibility is a fundamental concept of number theory and is one of the main ideas that sets it apart from other branches of mathematics. The main approach to divisibility questions is through the arithmetic of remainders, or the theory of congruences as it is now commonly known. The concept was first introduced by Carl Friedrich Gauss (1777-1855) in his *Disquisitiones Arithmeticae*; this monumental work, which appeared in 1801 when Gauss was 24 years old, laid the foundations of modern number theory.

We say that a is *congruent to* b modulo m, and we write

$$a \equiv b \pmod{m},$$

if m divides the difference $a - b$; that is, provided $a - b = km$ or $a = b + km$ for some integer k. If $m \nmid (a - b)$, then we say that a is *incongruent to* b modulo m and in this case we write $a \not\equiv b \pmod{m}$.

For example,

$$\begin{aligned} 3 &\equiv 24 \pmod{7} \quad \text{since } 7|(3-24), \\ 19 &\equiv -2 \pmod{7} \quad \text{since } 7|(19+2), \\ -15 &\equiv -64 \pmod{7} \quad \text{since } 7|(-15+64). \end{aligned}$$

The number m is called the *modulus* of the congruence. Congruences with the same modulus behave in many ways like ordinary equations. In particular, if

$$a \equiv b (\text{mod } m) \text{ and } c \equiv d (\text{mod } m),$$

then

$$a \pm c \equiv b \pm d (\text{mod } m) \text{ and } ac \equiv bd (\text{mod } m).$$

A warning is in order here. It is not always possible to divide congruences. If $ac \equiv bc \pmod{m}$, it need not be true that $a \equiv b \pmod{m}$. For example, we have $15 \cdot 2 \equiv 20 \cdot 2 \pmod{10}$, but $15 \not\equiv 20 \pmod{10}$. Even more distressing is that we can have $ab \equiv 0 \pmod{m}$ with $a \not\equiv 0 \pmod{m}$ and $b \not\equiv 0 \pmod{m}$. For example, $6 \cdot 4 \equiv 0 \pmod{12}$, while clearly $6 \not\equiv 0 \pmod{12}$ and $4 \not\equiv 0 \pmod{12}$. However, it is permissible to cancel c from the congruence $ac \equiv bc \pmod{m}$ provided that c and m do not have common factors, that is $\gcd(c, m) = 1$.

Let a be an integer. For any positive integer m, by the division algorithm, we have

$$a = mq + r \text{ where } 0 \leq r \leq m-1,$$

and clearly $a \equiv r \pmod{m}$. The number r is called the *least positive residue* modulo m. Hence, every a is congruent modulo m to one and only one of the integers in the set $\{0, 1, 2, ..., m-1\}$, namely the (unique) remainder when divided by m. (Hence the justification of Gauss' phrase *arithmetic of remainders*.) It should be clear now that $a \equiv b \pmod{m}$ if and only if a and b have the same remainders when divided by m. We say that a and b are in the same *equivalence class* modulo m if they have the same remainder. We can think of $\equiv$ as behaving almost exactly like $=$ if we do not make a fuss over the difference between numbers in a particular equivalence class. Hence modulo 10 we see very little difference, so to speak, between 2 and 12 and 202 and -3008.

We will now see how congruences can be used to solve problems that otherwise might be cumbersome to solve. First note that we can make repeated use of the result that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ imply $a \pm c \equiv b \pm d \pmod{m}$ and $ac \equiv bd \pmod{m}$. For example, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$. Hence, for example,

$$10^{17} \equiv 1^{17} \equiv 1 \pmod{9},$$
$$10^{17} \equiv (-1)^{17} \equiv -1 \equiv 10 \pmod{11}.$$

Note that 10^{17} is quite a large number, but we found the remainders quite effortlessly! We quote the limerick by Martin Gardner about the modulus 10:

> *There was a young fellow named Ben*
> *Who could only count modulo ten.*
> *He said, "When I go*
> *Past my last little toe,*
> *I shall have to start over again."*

Problem 1 *Prove that a number is divisible by 3 if and only if the sum of its digits is divisible by 3, and that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.*

Solution: We prove the rule for divisibility by 9. Let $N = \sum_{k=0}^{m} a_k 10^k$, where $0 \leq a_k \leq 9$ and $a_m \neq 0$. Clearly $N \equiv \sum_{k=0}^{m} a_k \pmod{9}$ since $10^k \equiv 1^k \equiv 1 \pmod{9}$. Hence $N \equiv 0 \pmod{9}$ if and only if $\sum_{k=0}^{m} a_k \equiv 0 \pmod{9}$. □

Note that we are instinctively using the following rules for congruences which really need proof: for any modulus m, $a \equiv b$ implies $b \equiv a$, and $a \equiv b$, $b \equiv c$, imply $a \equiv c$.

Problem 2 *Given the number 2492, double the units digit and subtract it from the number formed by the other digits. We get* $249 - 2 \times 2 = 245$. *Repeating this algorithm we get* $24 - 2 \times 5 = 14$. *Since 14 is clearly divisible by 7, the original number 2492 must be divisible by 7. Prove this rule for checking divisibility by 7.*

Solution: Let $N = \sum_{k=0}^{m} a_k 10^k$ where $0 \le a_k \le 9$ and $a_m \neq 0$. Then

$$\begin{aligned} N &= 10\left(\sum_{k=1}^{m} a_k 10^{k-1}\right) + a_0 \\ &\equiv 10\left(\sum_{k=1}^{m} a_k 10^{k-1}\right) - 20a_0 \pmod 7 \\ &\equiv 10\left(\sum_{k=1}^{m} a_k 10^{k-1} - 2a_0\right) \pmod 7. \end{aligned}$$

Hence $N \equiv 0 \pmod 7$ if and only if

$$\sum_{k=1}^{m} a_k 10^{k-1} - 2a_0 \equiv 0 \pmod 7$$

since $(10, 7) = 1$. □

Problem 3 *Prove that every odd integer other than a multiple of 5 has some multiple that is a string of 1's (called* a repunit*).*

Solution: We will leave the general proof to the reader. We will prove that 7 has a multiple of the form $1111\cdots$. The first $7 + 1$ repunit numbers are

$$1, 11, 111, 1111, 11111, 111111, 1111111, 11111111.$$

The residues (remainders) of these numbers modulo 7 are 1, 4, 6, 5, 2, 0, 1, and 4. Since there are eight numbers, we can apply the pigeon-hole principle: the pigeon-holes are labelled with the seven distinct residues modulo 7, and the pigeons are labelled with the 8 repunit residues; that is, we have one more pigeon than pigeon-holes, so two pigeons must share the same hole. So by the pigeon-hole principle, we must have at least two numbers with the same residue (mod 7). In this instance there are two such pairs. The smallest pair is 1 and 1111111. The difference is 1111110, which must be a multiple of 7. Since $7 \nmid 10$, we can divide by 10. Then $111111 = 7 \times 15873$ is a multiple of 7. □

Problem 4 *If a and b are odd integers, prove that* $a^2 + b^2$ *is never a square.*

Solution: For any integer c,

$$c^2 \equiv 0^2, 1^2, 2^2 \text{ or } 3^2 \pmod 4.$$

That is, $c^2 \equiv 0$ or $1 \pmod 4$. The odd squares can only be congruent to 1 modulo 4. Hence $a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4$. But 2 is not a square modulo 4. □

Problem 5 *Prove that* $a^2 - 11b^2 = 13$ *has no integer solutions.*

Solution: Modulo 11 we have for any solution a and b that $a^2 \equiv 13 \equiv 2 \pmod{11}$. But the squares modulo 11 are 0, 1, 4, 9, 5, and 3. The number 2 is not in this list! □

These so-called *Pell* equations have infinitely many solutions in many cases. For example, the equation $a^2 - 1141b^2 = 1$ has infinitely many positive integer solutions, the smallest one being $a = 1,036,782,394,157,223,963,237,125,215$ and $b = 30,693,385,322,765,657,197,397,208$ (26 digits).

Problem 6 *Prove that* $30|ab(a^4 - b^4)$ *for every pair of integers* a *and* b.

Solution: The most efficient way to solve this problem seems to be by using congruences modulo 2, 3, and 5. Consider each number in turn. For example, for the modulus 5, either $5|a$ or $5|b$ or, by checking the numbers $a \equiv 1$, 2, 3, and 4 (mod 5), we have $a^4 \equiv 1 \pmod{5}$. Similarly for b. Hence $a^4 - b^4 \equiv 1 - 1 \equiv 0 \pmod{5}$. That is, $5|(a^4 - b^4)$. □

Don Rideout is a retired math professor from Memorial University of Newfoundland. He can be reached via `drideout@mun.ca`.

Contact us

We welcome feedback on *MathemAttic* as the newest addition to *Crux*.

If you have questions, comments or ideas, please feel free to email editors at `MathemAttic@cms.math.ca`.