PRIMES Math Problem Set: Solutions

PRIMES

2020

Solution to General Math Problems

Problem G1

Let $n \geq 4$ be an integer. We wish to arrange the numbers $1, \ldots, n$ in a circle so that any two consecutive numbers sum to a prime number. For example, $(1, 2, 3, 4)$ would be a valid arrangement when $n = 4$.

(a) Is there an odd $n \geq 5$ for which this is possible?

(b) For each of $n = 6$, $n = 8$, $n = 10$, determine whether this is possible.

Solution

We first show the request is impossible for all odd $n \geq 5$. Indeed, in this case more than half the numbers in the circle are odd, and therefore there must exist two adjacent odd numbers. They add to an even number greater than 2, which is necessarily not prime.

We now give constructions for $n = 6$, $n = 8$, $n = 10$. They are:

- $(1, 4, 3, 2, 5, 6)$
- $(1, 6, 7, 4, 3, 8, 5, 2)$.
- $(1, 6, 7, 4, 3, 8, 5, 2, 9, 10)$.

In summary, the answer to (a) is no, the answer to (b) is yes for all three.

Problem G2

Consider pairs (a, b) of positive integers where b is not a perfect square and $a^2 > b$. Let

$$q = \sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}.$$

(a) Assume $(a, b) = (17943, 321185624)$. Show that q is rational and determine its value.

(b) Find another pair (a, b) as above for which q is rational.

(c) Determine whether there are infinitely many pairs (a, b) for which q is rational.

(d) Is it possible to find (a, b) such that q is rational but not an integer?

Solution

For all parts we will rewrite the equation as

$$q^2 = 2a + 2\sqrt{a^2 - b}.$$

(a): A calculation gives $q^2 = 2(17943 + \sqrt{765625}) = 2(17943 + 875) = 37636 = 194^2$. Thus $q = 194$ as, clearly, $q > 0$.

(b): Another such pair is $(a, b) = (6, 32)$ which gives $q^2 = 2(6 + \sqrt{4}) = 16$, hence $q = 4$.

(c): Let $n \geq 2$ be any integer. If we take $a = 2n^2 - 1$, $b = (2n^2 - 1)^2 - 1$ then we get $q^2 = (2n)^2$, or $q = 2n$.

(d): No, if q is rational it must be an integer. We make use of the following lemma: if t is a rational number and t^2 is an integer, then t is an integer. (This follows from the fact that if $t = \frac{m}{n}$ in lowest terms, and n^2 divides m^2, then n divides m).

According to the displayed equation, when q is rational it means $\sqrt{a^2 - b}$ is a rational, so by the lemma (with $a^2 - b$ being an integer), it follows $\sqrt{a^2 - b}$ is an integer. Thus q^2 is an integer, and since q is rational, the lemma applies again to give q is an integer.

Problem G3

Three distinct points are chosen on the parabola $y = x^2$, determining a triangle Δ.

(a) Express the area of Δ as a function of the three slopes of the sides of Δ.

(b) Determine the largest possible area of Δ, given that all slopes of sides of Δ have absolute value at most m.

Solution

(a): If (r, r^2), (s, s^2), (t, t^2) are the three points, then the slopes are $a = s + t$, $b = t + r$, $c = r + s$ respectively. Moreover the (signed) area of the triangle is given by

$$\frac{1}{2} \det \begin{bmatrix} 1 & r & r^2 \\ 1 & s & s^2 \\ 1 & t & t^2 \end{bmatrix} = \frac{(r-s)(s-t)(t-r)}{2} = \frac{(b-a)(c-b)(a-c)}{2}.$$

(b): WLOG let us assume $m \geq a \geq b \geq c \geq -m$; then note that

$$(a-b)(b-c)(a-c) \leq \left(\frac{a-c}{2}\right)^2 \cdot (a-c) \leq 2m^3$$

with equality when $a = m$, $b = 0$, $c = -m$. Thus, we conclude the area is at most m^3, achieved at $(0, 0)$, (m, m^2) and $(-m, m^2)$.

Problem G4

Let k be a positive integer. A 3×3 matrix M with integer entries is given. It turns out that each of the four continuous 2×2 submatrices has determinant 1. (These are the four minors obtained by deleting either the first row or last row, and either the first column or last column.) Moreover, the center entry is equal to k.

Given this information, find all possible values of $\det M$, in terms of k.

Solution

If $k = 0$ then $\det M$ may take any integer value. Indeed, let n be any integer and let

$$M = \begin{bmatrix} n & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

Then $\det M = n$.

On the other hand, we claim that if $k \neq 0$ then $\det M = 0$. Indeed, we may write the matrix as

$$M = \begin{bmatrix} \frac{ab+1}{k} & a & \frac{ad-1}{k} \\ b & k & d \\ \frac{cb+1}{k} & c & \frac{cd-1}{k} \end{bmatrix}$$

for some integers a, b, c, d. Notice that the sum of the first and last column is equal to $\frac{b+d}{k}$ times the second column. This implies $\det M = 0$. (And such a matrix M may be constructed by choosing $b = d = 1$ and $a = c = k - 1$, or indeed any values of a, b, c, d, with $ab \equiv cb \equiv -1 \pmod{k}$ and $ad \equiv cd \equiv 1 \pmod{k}$.)

Note that the condition about integer entries is a red herring; it is never used in any real way.

Problem G5

Let n be a positive integer and let $S = \{1, \dots, n\}$. We choose three subsets A, B, C of S uniformly at random (from the 2^n possible subsets), with replacement.

(a) Find the expected value of $|A \cap B \cap C|$.

(b) Find the expected value of $|A \cap B| \cdot |B \cap C|$.

Solution

For (a), each element appears in $A \cap B \cap C$ with probability $1/8$, so linearity of expectation then gives an answer of $n/8$.

For (b): suppose B is a fixed set of k elements. Conditioned on this, $|A \cap B|$ and $|C \cap B|$ are independent random variables with expected value $k/2$. Thus $|A \cap B| \cdot |B \cap C|$ has expected value $k^2/4$. Thus, the answer we seek is

$$2^{-n} \cdot \frac{1}{4} \cdot \sum_{k=0}^{n} k^2 \cdot \binom{n}{k}.$$

We now claim the well known identity

$$\sum_{k=0}^{n} k^2 \cdot \binom{n}{k} = (n^2 + n) \cdot 2^{n-2}. \qquad (\star)$$

The equation $(\star)$ can be proven by generating functions, or by Vandermonde's identity (writing $k^2 = 2\binom{k}{2} + \binom{k}{1}$). For completeness, here is a self-contained combinatorial proof: the left-hand side counts the number of ways to choose a subset S of k elements from $\{1, \dots, n\}$ and then pick an ordered pair (a, b) of elements from that subset. This could be counter in a different way: the number of pairs with $a = b$ is $n \cdot 2^{n-1}$ by picking $a = b$ first and then the rest of S; there are $n(n-1) \cdot 2^{n-2}$ ways to pick an (a, b) with $a \neq b$ and then the rest of S. Adding gives $(\star)$.

Putting everything together, we find the answer is $\frac{n^2+n}{16}$.

Problem G6

A robot starts at the point 0 on a number line. Thereafter, if it is at the number n, then

- it goes to $n+1$ with probability 1/2,
- it goes to $n-1$ with probability 1/3,
- it goes to $n-2$ with probability 1/6.

Determine the probability the robot ever reaches 1. You may take for granted the probability this occurs is not 1.

Solution

Let p_n be the probability the robot reaches 1 if the robot is stationed at n. Then we have the recursion

$$p_n = \frac{1}{2}p_{n+1} + \frac{1}{3}p_{n-1} + \frac{1}{6}p_{n-2}$$

with the boundary condition $p_1 = 1$.

Since we are given $p_0 < 1$, this implies $\lim_{n\to-\infty} p_n = 0$, since $p_n < p_0^{|n|+1}$; one has to manage to increment by $+1$ from the starting point at least $n+1$ times.

The characteristic polynomial of this recursion is

$$\frac{1}{2}t - 1 + \frac{1}{3}t^{-1} + \frac{1}{6}t^{-2} = 0$$

and solving gives $t = 1$ and $t = \frac{1}{6}(3 \pm \sqrt{21})$. So p_n must take the form

$$p_n = c_1 \cdot 1 + c_2 \cdot \left(\frac{1}{6}(3+\sqrt{21})\right)^n + c_3 \cdot \left(\frac{1}{6}(3-\sqrt{21})\right)^n$$

for some constants c_1, c_2, c_3. Taking $n \to -\infty$ we get $c_1 = c_3 = 0$, and taking $n = 1$ gives $c_2 = \left(\frac{1}{6}(3+\sqrt{21})\right)^{-1}$. Consequently, we must have the closed form

$$p_n = \left(\frac{1}{6}(3+\sqrt{21})\right)^{n-1}.$$

In particular,

$$p_0 = \left(\frac{1}{6}(3+\sqrt{21})\right)^{-1} = \frac{\sqrt{21}-3}{2} \approx 0.791$$

which is the answer.

Problem G7

Let n be a positive integer. An $n \times n$ board is given, and some rooks are placed on the board. In a move, any rook may capture another rook in the same row or column (i.e. if rook R is in the same row or column as rook R', then R' is removed and R takes its place). This continues until no more captures are possible; the resulting configuration is called peaceful.

(a) Describe an algorithm to compute, in $O(n^2)$ time, the maximum number of captures that can be made before reaching a peaceful configuration.

(b) Describe an algorithm to compute, in $O(n^3)$ time, the minimum number of captures that can be made before reaching a peaceful configuration.

If you use a standard or well-known algorithm as part of your solution, you do not need to describe the exact steps of the algorithm itself, but you should reference what the algorithm does, give either a name or citation, and state on the runtime.

Solution

In both parts, note that we can re-define the operation so that if rook R is in the same row or column as R', then we can just remove R, rather than removing R' and having R take its place. This eliminates the need to have rooks move across the board.

(a): Construct a graph G whose vertices are rooks, and whose edges join rooks in the same row or column. We claim the minimum number of rooks that remain is equal to the number of connected components of G. Indeed, as we delete vertices of G, the number of connected components cannot increase. Moreover, it's possible to never decrease the number of connected components either, by taking a spanning tree of each component, and only deleting leaves.

Thus, the algorithm only needs to compute the number of connected components of a given graph G. It's well known this can be done in time linear in the number of vertices, i.e. in $O(n^2)$ time.

(b): This time, we are looking for the set S of rooks of largest size, such that no two rooks are in the same row or column. To this end, we construct a bipartite graph H such that the left vertices are rows, right vertices are columns, and we draw an edge between any row/column pair that intersect at a rook. Then sets S as described correspond to matchings of H, and we are looking for the largest possible matching of H. The Ford-Fulkerson algorithm then gives us an algorithm whose runtime is $O(v(H) \cdot e(H)) = O(n^3)$.

Solution to Advanced Math Problems

Problem M1

There are six towers which are each 24 blocks tall. Bob the Builder wishes to merge them into a tower which is 144 blocks tall.

In a move, Bob may take a block from any tower (say with a blocks) and move it on top of any other tower (say with b blocks), as long as $a \leq b$. Due to gravity, the effort of doing so takes Bob $b - a + 2$ hours. Determine the minimum amount of time it takes Bob to construct a tower of height 144.

Solution

At each point in time, let k be the number of moves, and t the amount of time spent; and let a, b, c, d, e, f be the number of blocks in each towers.

The main idea is that the quantity

$$S = 2k - 2t + a^2 + b^2 + c^2 + d^2 + e^2 + f^2$$

does not change after each step.

Initially, we have $S = 24^2 \cdot 6$. At the end, we have $S = 144^2 + 2k - 2t$; and thus we have $2t - 2k = 144^2 - 24^2 \cdot 6 = 17280$ so $t = 8640 + k$.

We have $k \geq 120$ for obvious reasons; and this can be achieved by simply taking the second tower and moving all the blocks to the first, then all the blocks from the third to the first, and so on. Therefore the minimum amount of time required is 8760 hours, i.e. exactly one year.

Problem M2

Let $f\colon [0,1] \to \mathbb{R}$ be a strictly increasing function which is differentiable in $(0,1)$. Suppose that $f(0) = 0$ and for every $x \in (0,1)$ we have

$$\frac{f'(x)}{x} \geq f(x)^2 + 1.$$

How small can $f(1)$ be?

Solution

We claim the answer is $f(1) \geq \tan(1/2)$. This is achieved for example by $f(x) = \tan(x^2/2)$.

To show this is optimal, assume that $f\colon [0,1] \to [0, \tan(1/2)]$, and let $g(x) = \arctan(f(x))$, which is defined and also differentiable over $(0,1)$. By hypothesis,

$$g'(x) = \frac{f'(x)}{f(x)^2 + 1} \geq x$$

for all $0 < x < 1$. Consequently, $g(x) \geq x^2/2$ for all $0 < x < 1$ (say by mean value theorem), whence $g(1) \geq 1/2$, so $f(1) \geq \tan(1/2)$.

Problem M3

Let n be a fixed positive integer and consider the vector space V of real polynomials of degree at most n. We define the map $T\colon V \to V$ by

$$f(x) \mapsto \frac{d}{dx}\left[(x+1)^{n+1} \cdot f\left(\frac{1}{x+1}\right)\right].$$

Is T a linear map? If so, compute its determinant.

Solution

The map T is linear because precomposition with $x \mapsto \frac{1}{x+1}$, multiplication by $(x+1)^{n+1}$ and finally differentiation are all linear maps on the space of rational functions.

We now express T in matrix form. We take $\{1, x, \dots, x^n\}$ as a basis. Then,

$$\begin{aligned}
T(1) &= \frac{d}{dx}(x+1)^{n+1} = (n+1)(x+1)^n \\
T(x) &= \frac{d}{dx}(x+1)^{n} = n(x+1)^{n-1} \\
T(x^2) &= \frac{d}{dx}(x+1)^{n-1} = (n-1)(x+1)^{n-2} \\
&\vdots \\
T(x^n) &= \frac{d}{dx}(x+1)^{1} = 1 \cdot (x+1)^0.
\end{aligned}$$

Thus when written as a matrix we get an $(n+1)\times(n+1)$ matrix

$$T = \begin{bmatrix}
(n+1)\binom{n}{0} & n\binom{n-1}{0} & (n-1)\binom{n-2}{0} & \dots & 3 & 2 & 1 \\
(n+1)\binom{n}{1} & n\binom{n-1}{1} & (n-1)\binom{n-2}{1} & \dots & 6 & 2 & 0 \\
(n+1)\binom{n}{2} & n\binom{n-1}{2} & (n-1)\binom{n-2}{2} & \dots & 3 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
(n+1)\binom{n}{n-2} & n\binom{n-1}{n-2} & (n-1)\binom{n-2}{n-2} & \dots & 0 & 0 & 0 \\
(n+1)\binom{n}{n-1} & n\binom{n-1}{n-1} & 0 & \dots & 0 & 0 & 0 \\
(n+1)\binom{n}{n} & 0 & 0 & \dots & 0 & 0 & 0
\end{bmatrix}$$

Since all nonzero entries of the matrix lie above the antidiagonal, its determinant is equal to the product of the antidiagonal entries, times the sign of the permutation $(n+1, n, n-1, \dots, 1)$, which has $\binom{n+1}{2}$ inversions. In other words, it equals $(n+1)! \cdot (-1)^{\binom{n+1}{2}}$.

Problem M4

Let G be a finite group and let $A = \mathrm{Aut}(G)$ denote its automorphism group.

(a) If $|G| = 1048576$, can it happen that $|A|$ is divisible by 1048575?

(b) If $|G| = 1048572$, can it happen that $|A|$ is divisible by 1048571?

Solution

The answer to (a) is yes: take $G = \mathbb{F}_2^{20}$. Then $A = \mathrm{GL}_{20}(\mathbb{F}_2)$ which is known to have $\prod_{i=0}^{19}(2^{20} - 2^i)$ elements, and this is evidently divisible by 1048575.

The answer to (b) is no. We have a group G of order $p+1$ having $|A|$ divisible by p, where p is prime. We claim this can never occur. Indeed, if so there exists an automorphism σ of G with order p (by Cauchy theorem, say). Then this must fix the identity of G and cycle the remaining elements of G. This implies all non-identity elements of G have the same order. In particular $|G|$ must be a prime power, which it is not.

Problem M5

Recall that a polynomial is *monic* if its leading coefficient is 1. We say an integer $n \geq 2$ is *chaotic* if for any monic nonconstant polynomial $f(x)$ with positive integer coefficients, the set

$$\{f(1), f(2), \dots, f(n)\}$$

contains fewer than $10^{\deg f} \cdot \frac{n}{\log n}$ prime numbers. Are there finitely many chaotic integers?

(Possible hint: use the prime number theorem for arithmetic progressions.)

Solution

The answer is yes: we prove all sufficiently large integers n are not chaotic.

We fix a large number A as the product of the first several primes — enough so that $A/\varphi(A) > 303$. Then pick a constant r such that $-r \pmod p$ is not a quadratic residue modulo any prime dividing A. Note that the constants A and r do not depend on n. According to the prime number theorem for arithmetic progressions (PNTAP), for any $1 \leq a \leq A$ with $\gcd(a, A) = 1$, the number of $a \pmod A$ primes which are at most x is is $(\frac{1}{\varphi(A)} + o(1))\frac{x}{\log x}$, uniformly in a.

Let n be any integer. Our idea is to pick our polynomial of the form

$$f(x) = (x+1)^2 + Ak + r$$

for some suitable integer $k > 0$. Let $N = n^3$. Consider the following $n \times N$ table:

$$\begin{bmatrix} 4+A+r & 9+A+r & 16+A+r & \dots & (n+1)^2+A+r \\ 4+2A+r & 9+2A+r & 16+2A+r & \dots & (n+1)^2+2A+r \\ 4+3A+r & 9+3A+r & 16+3A+r & \dots & (n+1)^2+3A+r \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 4+NA+r & 9+NA+r & 16+NA+r & \dots & (n+1)^2+NA+r. \end{bmatrix}$$

Now, the number of primes in each column is equal to

$$\left(\frac{1}{\varphi(A)} + o(1)\right)\frac{AN}{\log(AN)} - O(n^2) = \left(\frac{A}{3\varphi(A)} + o(1)\right)\frac{N}{\log n} > (101 + o(1))\frac{N}{\log n}$$

with the $-O(n^2)$ term coming from some small primes we didn't count when applying PNTAP. It follows the number of primes in the table overall equals

$$(101 + o(1))\frac{Nn}{\log n}.$$

Thus, if n is large enough, the number of primes in the table is greater than $\frac{100Nn}{\log n}$, and thus for sufficiently large n there exists some row with at least $\frac{100n}{\log n}$ primes in it. This gives us the required polynomial f.

Remark M5.1. This problem was based on a question from Miklos Schweitzer 1990 which was proposed then by I. Z. Ruzsa.

Note the subtlety in applying PNTAP — the error term in PNTAP for $\{a, a+A, a+2A, a+3A, \dots\}$ depends on the choice of a. If we tried directly apply PNTAP to the columns of the table, then the implicit error terms would change as we moved across columns, breaking the proof. Thus in our work we have to ensure we apply the theorem only $O(1)$ times. This is why we need $N = n^3$, so that we only apply PNTAP for starting terms $1 \leq a \leq A$ in the arithmetic progressions and can safely ignore the first $O(n^2)$ small terms which do not appear in a column.

Problem M6

Fix an additive abelian group G. Say a family $\mathcal{I}$ of *finite* subsets of G is G*-admissible* if the following properties hold:

- if $A \in \mathcal{I}$ and $g \in G$, then $g + A = \{g + a \mid a \in A\}$ is also in $\mathcal{I}$;
- whenever $A, B \in \mathcal{I}$, the symmetric difference
$$A \triangle B = \{x \mid (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A)\}$$
is also in $\mathcal{I}$.

If $A \subseteq G$ is finite, let $\overline{A}$ denote the smallest admissible family containing A.

(a) Is every $\mathbb{Z}$-admissible set of the form $\overline{A}$ for some A?

(b) Describe all $\mathbb{Z}$-admissible sets.

(c) For each $n = 2, 3, \ldots, 9$ compute the number of $\mathbb{Z}/n\mathbb{Z}$-admissible sets.

(d) What can you say about $\mathbb{Z}/n\mathbb{Z}$-admissible sets for general n?

Solution

We first tackle (a) and (b) and fix $G = \mathbb{Z}$. We identify each finite subset $A \in \mathcal{I}$ with a Laurent polynomial with $\mathbb{F}_2$ coefficients by

$$A \mapsto p_A = \sum_{n \in A} x^n \in \mathbb{F}_2[x, x^{-1}].$$

Thus we have identified families of finite sets with subsets of the ring $\mathbb{F}_2[x, x^{-1}]$.

In this way, an admissible family $\mathcal{I}$ corresponds to an *ideal* I of the ring $\mathbb{F}_2[x, x^{-1}]$; the first condition implies that I is closed under multiplication by x and x^{-1}, while the second condition implies that I is closed under addition.

However, since $\mathbb{F}_2[x, x^{-1}]$ is a principal ideal domain. (In particular, (a) is yes.) It follows that the ideal I is of the form $I = (p)$ for some polynomial $p \in \mathbb{F}_2[x, x^{-1}]$; and so $\mathcal{I}$ is in bijection with finite subsets A of $\mathbb{Z}$ modulo translation, according to $I = (p_A)$. This completes the description of admissible sets for $R = \mathbb{Z}$.

We proceed to (c) and (d) with $G = \mathbb{Z}/n\mathbb{Z}$. In the same way as above, we see that G-admissible sets are identified with ideals

$$I \subseteq \mathbb{F}_2[x]/(x^n - 1).$$

In turn, these correspond to ideals of $\mathbb{F}_2[x]$ which contain $(x^n - 1)$.

However, since $\mathbb{F}_2$ is a field it follows that $\mathbb{F}_2[x]$ is a PID, so ideals of $\mathbb{F}_2[x]$ containing $x^n - 1$ are simply in bijection with factors of $x^n - 1$.

So the problem amounts to finding the number of factors of $x^n - 1$ in $\mathbb{F}_2[x]$. Taking advantage of the fact that $\mathbb{F}_2[x]$ is a unique factorization domain we just need to compute the irreducible factorizations of

$$x^n - 1 \pmod 2.$$

For $n = 2, \ldots, 9$ we can compute the answer directly as in the following table.

n	$x^n - 1 \pmod 2$ factorization	Answer
$n = 2$	$(x+1)^2$	3
$n = 3$	$(x+1)(x^2+x+1)$	4
$n = 4$	$(x+1)^4$	5
$n = 5$	$(x+1)(x^4+x^3+x^2+x+1)$	4
$n = 6$	$(x+1)^2(x^2+x+1)^2$	9
$n = 7$	$(x+1)(x^3+x+1)(x^3+x^2+1)$	8
$n = 8$	$(x+1)^8$	9
$n = 9$	$(x+1)(x^2+x+1)(x^6+x^3+1)$	8

For general n, if we write $n = 2^e t$ where t is an odd integer, then we have

$$x^n - 1 = \left(x^t - 1\right)^{2^e} \pmod 2$$

and $x^t - 1$ has no repeated factors (its derivative in $\mathbb{F}_2$ is tx^{t-1}). So the answer should be of the form $(2^e+1)^N$ where N is the number of irreducible factors of $x^t - 1$.