HMMT February 2020

February 15, 2020

Team Round

1. **[20]** Let n be a positive integer. Define a sequence by $a_0 = 1$, $a_{2i+1} = a_i$, and $a_{2i+2} = a_i + a_{i+1}$ for each $i \geq 0$. Determine, with proof, the value of $a_0 + a_1 + a_2 + \cdots + a_{2^n-1}$.

   Proposed by: Kevin Ren

   Answer: $\boxed{\frac{3^n+1}{2}}$

   Solution 1: Note that $a_{2^n-1} = 1$ for all n by repeatedly applying $a_{2i+1} = a_i$. Now let $b_n = a_0 + a_1 + a_2 + \cdots + a_{2^n-1}$. Applying the given recursion to every term of b_n except a_0 gives

$$\begin{aligned}
b_n =& a_0 + a_1 + a_2 + a_3 + \cdots + a_{2^n-1} \\
=& a_0 + a_2 + a_4 + \cdots + a_{2^n-2} + a_1 + a_3 + \cdots + a_{2^n-1} \\
=& a_0 + (a_0 + a_1) + (a_1 + a_2) + (a_2 + a_3) + \cdots + (a_{2^{n-1}-2} + a_{2^{n-1}-1}) \\
&+ a_0 + a_1 + a_2 + \cdots + a_{2^{n-1}-1} \\
=& 3a_0 + 3a_1 + 3a_2 + \cdots + 3a_{2^{n-1}-2} + 3a_{2^{n-1}-1} - a_{2^{n-1}-1} \\
=& 3b_{n-1} - 1.
\end{aligned}$$

   Now we easily obtain $b_n = \frac{3^n+1}{2}$ by induction.

   Solution 2: Define a binary string to be good if it is the null string or of the form $101010\ldots10$. Let c_n be the number of good subsequences of n when written in binary form. We see $c_0 = 1$ and $c_{2n+1} = c_n$ because the trailing 1 in $2n+1$ cannot be part of a good subsequence. Furthermore, $c_{2n+2} - c_{n+1}$ equals the number of good subsequences of $2n+2$ that use the trailing 0 in $2n+2$. We will show that this number is exactly c_n.

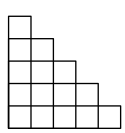
   Let s be a good subsequence of $2n+2$ that contains the trailing 0. If s uses the last 1, remove both the last 1 and the trailing 0 from s; the result s' will be a good subsequence of n. If s does not use the last 1, consider the sequence s' where the trailing 0 in $2n+2$ is replaced by the last 0 in n (which is at the same position as the last 1 in $2n+2$.) The map $s \mapsto s'$ can be seen to be a bijection, and thus $c_{2n+2} = c_n + c_{n+1}$.

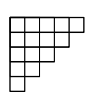
   Now it is clear that $a_n = c_n$ for all n. Consider choosing each binary string between 0 and $2^n - 1$ with equal probability. The probability that a given subsequence of length $2k$ is good is $\frac{1}{2^{2k}}$. There are $\binom{n}{2k}$ subsequences of length $2k$, so by linearity of expectation, the total expected number of good subsequences is

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \frac{\binom{n}{2k}}{2^{2k}} = \frac{(1+1/2)^n + (1-1/2)^n}{2} = \frac{3^n+1}{2^{n+1}}.$$

   This is equal to the average of $a_0, \ldots, a_{2^n-1}$, therefore the sum $a_0 + \cdots + a_{2^n-1}$ is $\frac{3^n+1}{2}$.

2. **[25]** Let n be a fixed positive integer. An n-staircase is a polyomino with $\frac{n(n+1)}{2}$ cells arranged in the shape of a staircase, with arbitrary size. Here are two examples of 5-staircases:





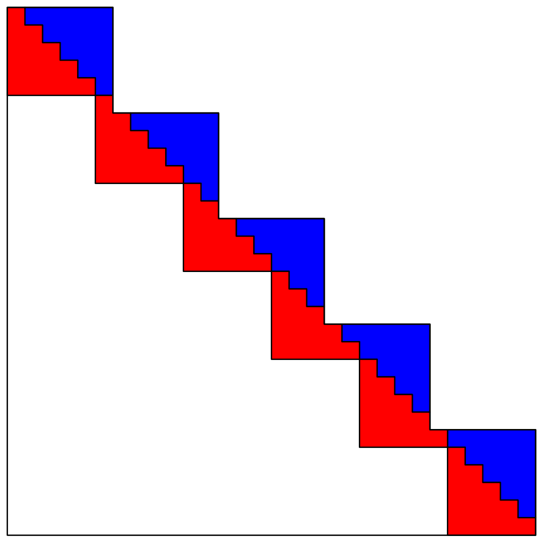
   Prove that an n-staircase can be dissected into strictly smaller n-staircases.

   Proposed by: James Lin

Solution 1: Viewing the problem in reverse, it is equivalent to show that we can use multiple n-staircases to make a single, larger n-staircase, because that larger n-staircase is made up of strictly smaller n-staircases, and is the example we need.

For the construction, we first attach two n-staircases of the same size together to make an $n \times (n+1)$ rectangle. Then, we arrange $n(n+1)$ of these rectangles in a $(n+1) \times n$ grid, giving an $n(n+1) \times n(n+1)$ size square. Finally, we can use $\frac{n(n+1)}{2}$ of these squares to create a larger n-staircase of $n^2(n+1)^2$ smaller staircases, so we are done.

Solution 2: An alternative construction using only $2n+2$ staircases was submitted by team Yeah Knights A. We provide a diagram for $n = 5$ and allow the interested reader to fill in the details.



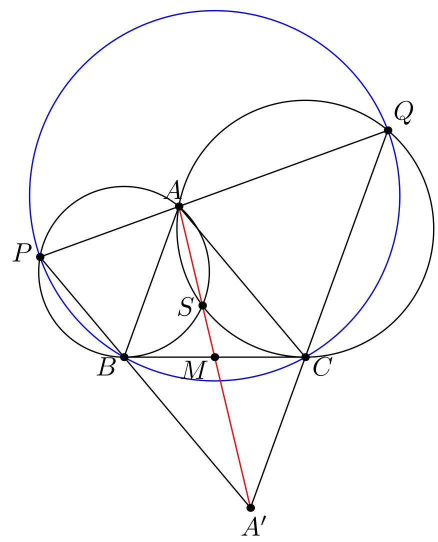
3. **[25]** Let ABC be a triangle inscribed in a circle ω and ℓ be the tangent to ω at A. The line through B parallel to AC meets ℓ at P, and the line through C parallel to AB meets ℓ at Q. The circumcircles of ABP and ACQ meet at $S \neq A$. Show that AS bisects BC.

   Proposed by: Andrew Gu

   Solution 1: In directed angles, we have

$$\measuredangle CBP = \measuredangle BCA = \measuredangle BAP,$$

   so BC is tangent to the circumcircle of ABP. Likewise, BC is tangent to the circumcircle of ACQ. Let M be the midpoint of BC. Then M has equal power $MB^2 = MC^2$ with respect to the circumcircles of ABP and ACQ, so the radical axis AS passes through M.



Solution 2: Since

$$\measuredangle CBP = \measuredangle BCA = \measuredangle BAP = \measuredangle CQP,$$

quadrilateral $BCQP$ is cyclic. Then AS, BP, and CQ concur at a point A'. Since $A'B \parallel AC$ and $A'C \parallel AB$, quadrilateral $ABA'C$ is a parallelogram so line ASA' bisects BC.

4. **[35]** Alan draws a convex 2020-gon $\mathcal{A} = A_1A_2\cdots A_{2020}$ with vertices in clockwise order and chooses 2020 angles $\theta_1, \theta_2, \ldots, \theta_{2020} \in (0, \pi)$ in radians with sum 1010π. He then constructs isosceles triangles $\triangle A_iB_iA_{i+1}$ on the exterior of $\mathcal{A}$ with $B_iA_i = B_iA_{i+1}$ and $\angle A_iB_iA_{i+1} = \theta_i$. (Here, $A_{2021} = A_1$.) Finally, he erases $\mathcal{A}$ and the point B_1. He then tells Jason the angles $\theta_1, \theta_2, \ldots, \theta_{2020}$ he chose. Show that Jason can determine where B_1 was from the remaining 2019 points, i.e. show that B_1 is uniquely determined by the information Jason has.

   Proposed by: Andrew Gu, Colin Tang

   Solution 1: For each i, let τ_i be the transformation of the plane which is rotation by θ_i counterclockwise about B_i. Recall that a composition of rotations is a rotation or translation, and that the angles of rotation add. Consider the composition $\tau_{2020} \circ \tau_{2019} \circ \cdots \circ \tau_1$, with total rotation angle 1010π. This must be a translation because $1010\pi = 505(2\pi)$. Also note that the composition sends A_1 to itself because $\tau_i(A_i) = A_{i+1}$. Therefore it is the identity. Now Jason can identify the map τ_1 as $\tau_2^{-1} \circ \tau_3^{-1} \circ \cdots \circ \tau_{2020}^{-1}$, and B_1 is the unique fixed point of this map.

   Solution 2: Fix an arbitrary coordinate system. For $1 \le k \le 2020$, let a_k, b_k be the complex numbers corresponding to A_k, B_k. The given condition translates to

$$e^{i\theta_k}(b_k - a_k) = (b_k - a_{k+1}). \qquad (1 \le k \le 2020)$$

   In other words

$$(e^{i\theta_k} - 1)b_k = e^{i\theta_k}a_k - a_{k+1},$$

   or

$$(e^{-i(\theta_{k-1}+\cdots+\theta_1)} - e^{-i(\theta_k+\cdots+\theta_1)})b_k = e^{-i(\theta_{k-1}+\cdots+\theta_1)}a_k - e^{-i(\theta_k+\cdots+\theta_1)}a_{k+1}.$$

   Summing over all k, and using the fact that

$$e^{-i(\theta_1+\cdots+\theta_{2020})} = 1,$$

we see that the right hand side cancels to 0, thus

$$\sum_{k=1}^{2020} (e^{-i(\theta_{k-1}+\cdots+\theta_1)} - e^{-i(\theta_k+\cdots+\theta_1)})b_k = 0.$$

Jason knows $b_2, \ldots, b_{2020}$ and all the θ_i, so the equation above is a linear equation in b_1. We finish by noting that the coefficient of b_1 is $1 - e^{-i\theta_1}$ which is non-zero, as $\theta_1 \in (0, \pi)$. Thus Jason can solve for b_1 uniquely.

Solution 3: Let $A_1A_2\cdots A_{2020}$ and $\tilde{A}_1\tilde{A}_2\cdots\tilde{A}_{2020}$ be two 2020-gons that satisfy the conditions in the problem statement, and let B_k, $\tilde{B}_k$ be the points Alan would construct with respect to these two polygons. It suffices to show that if $B_k = \tilde{B}_k$ for $k = 2, 3, \ldots, 2020$, then $B_1 = \tilde{B}_1$.

For $2 \le k \le 2020$, we note that

$$A_kB_k = A_{k+1}B_k, \quad \tilde{A}_kB_k = \tilde{A}_{k+1}B_k$$

Furthermore, we have the equality of directed angles $\angle A_kB_kA_{k+1} = \angle\tilde{A}_kB_k\tilde{A}_{k+1} = \theta_k$, therefore $\angle A_kB_k\tilde{A}_k = \angle A_{k+1}B_k\tilde{A}_{k+1}$. This implies the congruence $\triangle A_kB_k\tilde{A}_k \cong \triangle A_{k+1}B_k\tilde{A}_{k+1}$.

The congruence shows that $A_k\tilde{A}_k = A_{k+1}\tilde{A}_{k+1}$; furthermore, the angle from the directed segment $\overrightarrow{A_k\tilde{A}_k}$ to $\overrightarrow{A_{k+1}\tilde{A}_{k+1}}$ is θ_k counterclockwise. This holds for $k = 2, 3, \ldots, 2020$; we conclude that $A_1\tilde{A}_1 = A_2\tilde{A}_2$, and the angle from the directed segments $\overrightarrow{A_1\tilde{A}_1}$ to $\overrightarrow{A_2\tilde{A}_2}$ is

$$-\sum_{k=2}^{2020} \theta_k = \theta_1 - 1010\pi = \theta_1$$

counterclockwise.

Finally we observe that $A_1B_1 = A_2B_1$, and the angle from the directed segment $\overrightarrow{A_1B_1}$ to $\overrightarrow{A_2B_1}$ is θ_1 counterclockwise. This implies $\angle B_1A_1\tilde{A}_1 = \angle B_1A_2\tilde{A}_2$, so $\triangle A_1B_1\tilde{A}_1 \cong \triangle A_2B_1\tilde{A}_2$. Thus $\tilde{A}_1B_1 = \tilde{A}_2B_1$, and the angle from $\overrightarrow{\tilde{A}_1B_1}$ to $\overrightarrow{\tilde{A}_2B_1}$ is θ_1 counterclockwise. We conclude that $B_1 = \tilde{B}_1$.

5. **[40]** Let a_0, b_0, c_0, a, b, c be integers such that $\gcd(a_0, b_0, c_0) = \gcd(a, b, c) = 1$. Prove that there exists a positive integer n and integers $a_1, a_2, \ldots, a_n = a, b_1, b_2, \ldots, b_n = b, c_1, c_2, \ldots, c_n = c$ such that for all $1 \le i \le n$, $a_{i-1}a_i + b_{i-1}b_i + c_{i-1}c_i = 1$.

   Proposed by: Michael Ren

   Solution: The problem statement is equivalent to showing that we can find a sequence of vectors, each with 3 integer components, such that the first vector is (a_0, b_0, c_0), the last vector is (a, b, c), and every pair of adjacent vectors has dot product equal to 1.

   We will show that any vector (a, b, c) can be sent to $(1, 0, 0)$. This is sufficient, because given vectors (a_0, b_0, c_0) and (a, b, c), we take the sequence from (a_0, b_0, c_0) to $(1, 0, 0)$ and then add the reverse of the sequence from (a, b, c) to $(1, 0, 0)$.

   First, suppose that some two of a, b, c are relatively prime. Here we will suppose that a and b are relatively prime; the other cases are similar. If neither of a or b is 0, then by Bezout's identity, there exist p, q such that $|p|+|q| < |a|+|b|$ and $ap+bq = 1$, so we can send (a, b, c) to $(p, q, 0)$. (Finding such numbers can be done using the extended Euclidean algorithm.) Clearly p and q must also be relatively prime, so we can apply Bezout's identity repeatedly until we eventually have $(1, 0, 0), (-1, 0, 0), (0, 1, 0)$, or $(0, -1, 0)$. Now, starting from $(0, -1, 0)$, we can do $(0, -1, 0) \to (1, -1, 0) \to (1, 0, 0)$, and we can do something similar to convert $(-1, 0, 0)$ to $(0, 1, 0)$.

   Now suppose that no two of a, b, c are relatively prime. Let $f = \gcd(a, b)$. We claim that we can find x, y, z such that $axy + bx + cz = 1$. Notice that this is the same as $(ay + b)x + cz = 1$. Since

$\gcd(a,b,c)=1$, there exists y such that $\gcd(ay+b,c)=1$. Then by Bezout's identity, there exist x,z such that $(ay+b)x+cz=1$. Therefore, we can send (a,b,c) to (xy,x,z). Clearly x and z must be relatively prime, so we have reduced to the case above, and we can apply the process described above for that case.

At the end of this process, we will have $(1,0,0)$, $(0,1,0)$, or $(0,0,1)$. The second of these can be converted into $(1,0,0)$ by doing $(0,1,0)\to(1,1,0)\to(1,0,0)$, and a similar sequence shows the same for the third. Therefore, (a,b,c) can be sent to $(1,0,0)$.

6. **[40]** Let $n>1$ be a positive integer and S be a collection of $\frac{1}{2}\binom{2n}{n}$ distinct n-element subsets of $\{1,2,\ldots,2n\}$. Show that there exists $A,B\in S$ such that $|A\cap B|\le 1$.

Proposed by: Michael Ren

Solution 1: Assume for the sake of contradiction that there exist no such A, B. Pair up each subset with its complement, like so:

$$\begin{aligned}
\{1,2,3,\ldots,n\} &\leftrightarrow \{n+1,n+2,\ldots,2n\}\\
\{1,2,3,\ldots,n-1,n+1\} &\leftrightarrow \{n,n+2,\ldots,2n\}\\
\{1,2,3,\ldots,n-1,n+2\} &\leftrightarrow \{n,n+1,n+3,\ldots,2n\}\\
&\vdots
\end{aligned}$$

Note that for each pair, we can have at most one of the two in S. Since S has $\frac{1}{2}$ of the total number of subsets with size n, it must be that we have exactly one element from each pair in S. For any $s_0\in S$, none of the subsets that share exactly one element with s_0 can be in S, so their complements must be in S. This means that every subset with $n-1$ shared elements with s_0 must be in S. Without loss of generality, assume $\{1,2,3,\ldots,n\}\in S$. Then, $\{2,3,4,\ldots,n+1\}\in S$, so $\{3,4,5,\ldots,n+2\}\in S$. Continuing on in this manner, we eventually reach $\{n+1,n+2,\ldots,2n\}\in S$, contradiction.

Solution 2: Let $[2n]=\{1,2,\ldots,2n\}$. Consider the following cycle of $2n-1$ sets such that any two adjacent sets have an intersection of size 1:

$$\begin{aligned}
&\{1,2,3,\ldots,n\},\\
&\{1,n+1,n+2,\ldots,2n-1\},\\
&\{1,2n,2,3,\ldots,n-1\},\\
&\vdots\\
&\{1,n+2,n+3,\ldots,2n\}.
\end{aligned}$$

If S contains two adjacent elements of the cycle then we are done. For each permutation σ of $[2n]$, we can consider the cycle C_σ of sets obtained after applying σ, i.e. $\{\sigma(1),\sigma(2),\sigma(3),\ldots,\sigma(n)\}$ and so on. In total, each subset of $[2n]$ with size n appears $(2n-1)(n!)^2$ times across all the cycles C_σ, so

$$\sum_\sigma |C_\sigma\cap S| = |S|(2n-1)(n!)^2 = \frac{2n-1}{2}(2n)!$$

where the sum is over all $(2n)!$ permutations of $[2n]$. This means that on average across possible cycles, $\frac{2n-1}{2}$ of its elements are in S. Thus, if we select a cycle C_σ uniformly at random, with positive probability we will have $|C_\sigma\cap S|\ge n$, so two adjacent elements in this cycle will be in S. Therefore, there must exist some two subsets in S that share at most one element.

This proof will work under the weaker condition $|S|>\frac{n-1}{2n-1}\binom{2n}{n}$.

Remark. A family of sets such that $|A\cap B|\ge t$ for every pair of distinct sets A, B is called *t-intersecting*. Ahlswede and Khachatrian solved the problem of determining the largest k-uniform t-intersecting family. See "Katona's Intersection Theorem: Four Proofs" or "The Complete Intersection

Theorem for Systems of Finite Sets" for exact results.

7. **[50]** Positive real numbers x and y satisfy

$$\left|\left|\cdots\left|\left||x|-y\right|-x\right|\cdots-y\right|-x\right| \;=\; \left|\left|\cdots\left|\left||y|-x\right|-y\right|\cdots-x\right|-y\right|$$

where there are 2019 absolute value signs $|\cdot|$ on each side. Determine, with proof, all possible values of $\frac{x}{y}$.

Proposed by: Krit Boonsiriseth

Answer: $\boxed{\frac{1}{3}, 1, 3}$

Solution: Clearly $x=y$ works. Else WLOG $x<y$, define $d=y-x$, and define $f(z) := \left||z-y|-x\right|$ so our expression reduces to

$$f^{1009}(x) = \left|f^{1009}(0)-y\right|.$$

Now note that for $z \in [0,y]$, $f(z)$ can be written as

$$f(z) = \begin{cases} d-z, & 0 \le z \le d \\ z-d, & d < z \le y \end{cases}$$

Hence $f(f(z)) = f(d-z) = z$ for all $z \in [0,d]$. Therefore

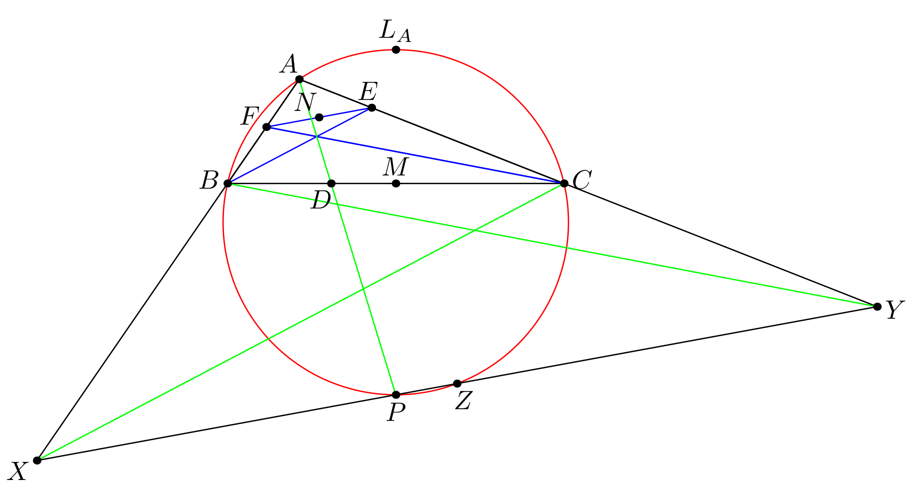
$$\left|f^{1009}(0)-y\right| = |f(0)-y| = x.$$

If $x>d$ then $f^{1009}(x)<x$ which is impossible (if $f^{1009}(x) \le d$ then the conclusion trivially holds, and if $f^{1009}(x)>d$ we must have $f^{1009}(x) = x-1009d<x$). Therefore $x \le d$, so $f^{1009}(x) = f(x) = d-x$ and we must have $d-x=x$. Hence $y=3x$ which is easily seen to work. To summarize, the possible values of $\frac{x}{y}$ are $\frac{1}{3}, 1, 3$.

8. **[50]** Let ABC be a scalene triangle with angle bisectors AD, BE, and CF so that D, E, and F lie on segments BC, CA, and AB respectively. Let M and N be the midpoints of BC and EF respectively. Prove that line AN and the line through M parallel to AD intersect on the circumcircle of ABC if and only if $DE=DF$.

Proposed by: Michael Ren

Solution 1:



Let X, Y be on AB, AC such that $CX \parallel BE$ and $BY \parallel CF$. Then $BX = BC = CY$. Let Z be the midpoint of XY. Then $\overrightarrow{MZ} = \frac{1}{2}(\overrightarrow{BX} + \overrightarrow{CY})$, which bisects the angle between BX and CY because they have the same length. Therefore $MZ \parallel AD$. Furthermore, by similar triangles we have

$$AE \cdot AX = AB \cdot AC = AF \cdot AY.$$

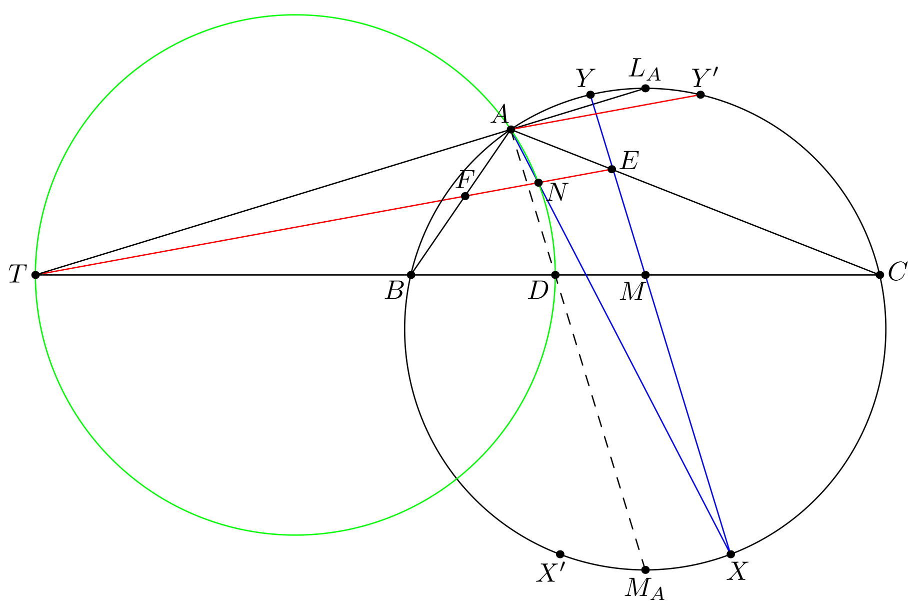
This rearranges to $\frac{AE}{AF} = \frac{AY}{AX}$, so $EF \parallel XY$. Therefore Z is the intersection of the lines in the problem statement. Then

$$\frac{\sin \angle BZX}{\sin \angle CZY} = \frac{BX \frac{\sin \angle ZBX}{XZ}}{CY \frac{\sin \angle ZCY}{YZ}} = 1$$

iff $Z \in (ABC)$, so XY is the external angle bisector of $\angle BZC$ iff $Z \in (ABC)$. Thus if $P = AD \cap XY$, $P \in (ABC)$ if $Z \in (ABC)$. Additionally the spiral similarity from BX to CY gives $L_A Z \perp XY$ where L_A is the midpoint of arc BAC, so if $P \in (ABC)$ then Z must be on (ABC) because $\angle L_A Z P = 90°$. Therefore $Z \in (ABC)$ iff $P \in (ABC)$.

From the previous length computation, we know that an inversion at A with radius $\sqrt{AB \cdot AC}$ composed with reflection about AD will send X and Y to E and F. We have $P \in (ABC)$ iff its image under the inversion is D, but since P was defined as $AD \cap XY$ this is true iff $(AEDF)$ is cyclic. Since ABC is scalene and $AE \neq AF$, this is true iff $DE = DF$.

Solution 2:



Let L_A be the midpoint of arc BAC and let M_A be diametrically opposite L_A. Let EF, AL_A, and BC meet at T so $\angle DAT = 90°$; note that $DE = DF$ iff $DN \perp EF$, which is equivalent to $(TAND)$ being cyclic. Let $AN \cap (ABC) = X$ and $XM \cap (ABC) = Y$, and let Y' be the reflection of Y over $L_A M_A$ with similarly X' the reflection of X over $L_A M_A$. We wish to show $N \in (TAD)$ iff $XY \parallel AM_A$.

We claim $AY' \parallel EF$. By projecting $-1 = (B, C; M, \infty) \stackrel{X}{=} (B, C; Y, X')$ and reflecting over $L_A M_A$, we find $(X, Y'; B, C) = -1$. Then projecting through A gives $(N, AY' \cap EF; F, E) = -1$, and since N is the midpoint of EF we find $AY' \parallel EF$.

Now $(TAND)$ cyclic iff $\measuredangle DAN = \measuredangle DTN$, and $\measuredangle DTN = \measuredangle YY'A$ by the parallel lines. But we have $\measuredangle DAN = \measuredangle M_A AX$, so arcs $M_A X$ and YA are equal iff $(TAND)$ is cyclic. Thus $XY \parallel AM_A$ iff $DE = DF$ as desired.

9. **[55]** Let $p > 5$ be a prime number. Show that there exists a prime number $q < p$ and a positive integer n such that p divides $n^2 - q$.

Proposed by: Andrew Gu

Solution 1: Note that the condition $p \mid n^2 - q$ just means that q is a quadratic residue modulo p, or that the Legendre symbol $\left(\frac{q}{p}\right)$ is 1. We use these standard facts about the Legendre symbol:

- If $p \equiv \pm 1 \pmod 8$, then $\left(\frac{2}{p}\right) = 1$.
- For an odd prime p,
$$\left(\frac{-1}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 4 \\ +1 & \text{if } p \equiv 1 \pmod 4 \end{cases}.$$
- Quadratic reciprocity: for distinct odd primes p and q,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \\ +1 & \text{otherwise} \end{cases}.$$

If p is a Fermat prime or Mersenne prime, then p is congruent to 1 or 7 modulo 8 respectively, since $p > 5$. In that case $q = 2$ works. Otherwise assume p is not a Fermat prime or Mersenne prime, so that $p - 1$ and $p + 1$ are not powers of 2.

If $p \equiv 1 \pmod 4$, then let q be an odd prime divisor of $p-1$, so that $p \equiv 1 \pmod q$. Then by quadratic reciprocity $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$.

If $p \equiv 3 \pmod 4$, then let q be an odd prime divisor of $p+1$, so that $p \equiv -1 \pmod q$. Either $q \equiv 1 \pmod 4$ so that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$ or $q \equiv 3 \pmod 4$ so that $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{-1}{q}\right) = 1$.

Solution 2: (Ankan Bhattacharya) We assume the same standard facts about quadratic residues as the previous solution.

If $p \equiv 1 \pmod 4$, then since $p > 5$, there exists an odd prime divisor q of $p - 4$, which gives
$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{4}{q}\right) = 1.$$

If $p \equiv 7 \pmod 8$, then we can take $q = 2$.

If $p \equiv 3 \pmod 8$, then by Legendre's three square theorem there exist odd a, b, c satisfying $p = a^2 + b^2 + c^2$. Since $p > 3$, these are not all equal and we may assume without loss of generality that $b \neq c$. Then $p - a^2 = b^2 + c^2$ has a prime divisor $q \equiv 1 \pmod 4$, which gives
$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{a^2}{q}\right) = 1.$$

Remark. For an odd prime number p, let $l(p)$ be the least prime number which is a quadratic residue modulo p and $h(-p)$ be the class number of the quadratic field $\mathbb{Q}[\sqrt{-p}]$. In the paper "The Least Prime Quadratic Residue and the Class Number" by Chowla, Cowles, and Cowles, the following results were proven:

- If $p > 5$ and $p \equiv 5 \pmod 8$, then $l(p) < \sqrt{p}$.
- If $p > 3$, $p \equiv 3 \pmod 8$, and $h(-p) > 1$, then $l(p) < \sqrt{p/3}$.
- If $p > 3$, $p \equiv 3 \pmod 8$, and $h(-p) = 1$, then $l(p) = \frac{p+1}{4}$.

The proofs of the second and third results require knowledge of binary quadratic forms.

10. **[60]** Let n be a fixed positive integer, and choose n positive integers $a_1, \ldots, a_n$. Given a permutation π on the first n positive integers, let $S_\pi = \{i \mid \frac{a_i}{\pi(i)} \text{ is an integer}\}$. Let N denote the number of distinct sets S_π as π ranges over all such permutations. Determine, in terms of n, the maximum value of N over all possible values of $a_1, \ldots, a_n$.

Proposed by: James Lin

Answer: $\boxed{2^n - n}$

Solution: The answer is $2^n - n$.

Let $D = (d_{ij})$ be the matrix where d_{ij} is 1 if i is a divisor of a_j and 0 otherwise. For a subset S of $[n]$, let D_S be the matrix obtained from D by flipping $(0 \leftrightarrow 1)$ every entry d_{ij} where $j \notin S$. Observe that $S = S_\pi$ if and only if $(D_S)_{\pi(i)i} = 1$ for all i.

To show that $N \leq 2^n - n$ we consider two cases. If all the rows of D are distinct, then there exist n different possibilities for S that set a row equal to zero. In this case, there is clearly no π so that $S_\pi = S$. Thus there are at most $2^n - n$ possible S_π. Otherwise, if two rows in D are the same, then choose an S_0 such that D_{S_0} has two zero rows. Then, the $n+1$ sets S that are at most "one element away" from S_0 are such that D_S only has one column with nonzero entries in those two rows. This makes it impossible for $S_\pi = S$ as well, so $N \leq 2^n - n - 1$.

Now we construct $N = 2^n - n$ by setting $a_j = j$. By Hall's marriage theorem, it suffices to prove the following:

Assuming that D_S has no completely-zero rows, given a set $I = \{i_1, i_2, \ldots, i_k\}$ there exist at least k values of j so that there exists an $i \in I$ so that $(D_S)_{ij} = 1$. Call such j admissible.

Without loss of generality assume $i_1 < i_2 < \cdots < i_k$.

Note that if $\{d_{ij} \mid i \in I\} = \{0, 1\}$, then j is admissible. Therefore the $k-1$ numbers $i_1, i_2, \ldots, i_{k-1}$ are admissible, since for $\alpha < k$, i_α divides i_α but i_k does not. So we only need to find one more admissible j. Assume that i_k is not admissible; now it must be the case that all the i_α are divisors of i_k.

At this point we note that the $k = 1$ case is easy, since no row of D_S is zero. Moreover, if $k = 2$, $\{(D_S)_{i_1 i_1}, (D_S)_{i_2 i_1}\} = \{0, 1\}$, so in the row with the zero there must be 1 somewhere, yielding a second admissible column.

In the case where $k \geq 3$, note that $i_1 \leq i_k/3$. Therefore $i_k - i_1 \notin I$, but i_1 divides $i_k - i_1$ and i_k does not. Thus we have found the last admissible column. Having exhausted all cases, we are done.