National Finals 2019 – Premier Division

Official Solution Key

April 28 — May 4, 2019

Time Limit: 2 hours.
Each problem is worth 7 points.

1. Kelvin the Frog and Alex the Kat are playing a game on an initially empty blackboard. Kelvin begins by writing a digit. Then, the players alternate inserting a digit anywhere into the number currently on the blackboard, including possibly a leading zero (e.g. 12 can become 123, 142, 512, 012, etc.). Alex wins if the blackboard shows a perfect square at any time, and Kelvin's goal is prevent Alex from winning. Does Alex have a winning strategy?

   Proposed by: Alexander Katz.

   Answer: $\boxed{\text{No}}$.

   Let n be the number currently on the blackboard. We claim that Kelvin can indefinitely avoid a perfect square with the following strategy: if $100n + 76$ is a perfect square, append a 3 to the end of the number. Otherwise, append a 7. Note that Kelvin thus plays a 7 on his first turn.

   Suppose that Alex can win the game with Kelvin following this strategy, and consider the turn on which Alex wins. At the beginning of this turn, the number on the blackboard ends in either a 3 or a 7. Since neither 3 nor 7 are quadratic residues modulo 10 (i.e. no perfect square ends in a 3 or a 7), Alex has not won at the beginning of his turn and cannot win by inserting a digit anywhere except the end of the number. Similarly, the only quadratic residues modulo 100 with a 3 or 7 in the tens place are 36 and 76, so Alex must win by appending a 6 to the end of the number.

   By Kelvin's strategy, if the number on the board ends with a 7, appending a 6 does not win. Therefore the number on the board must end with a 3, and Alex wins by appending a 6. In particular, both $100n + 36$ and $100n + 76$ are perfect squares; call these a^2 and b^2 respectively. Note that $n \geq 7$, so $b > a > 20$ and $b^2 - a^2 = (100n + 76) - (100n + 36) = 40$. But, we also have $b^2 - a^2 \geq 21^2 - 20^2 = 41$, which is a contradiction, so Alex cannot win against Kelvin's strategy.

   Remark 1. A common attempted strategy for Kelvin is to insert a 7 each turn, preserving the invariant that every other digit on the blackboard is 7. This is not a winning strategy: if Kelvin follows this strategy, Alex can get the number $767376 = 876^2$.

2. Let $n \geq 2$ be an even integer. Find the maximum integer k (in terms of n) such that 2^k divides $\binom{n}{m}$ for some $0 \leq m \leq n$.

   Proposed by: Kevin Ren.

   Answer: $\boxed{\lfloor \log_2 n \rfloor}$.

   Let $n = \overline{a_i a_{i-1} \cdots a_1 a_0}$ with $a_i = 1$ and $a_0 = 0$ be the base 2 representation of n. Let $v_2(m)$ denote the largest k such that $2^k | m$, and $s_2(m)$ be the number of ones in the binary representation of m. It is well-known that $v_2(n!) = n - s_2(n)$. So,

$$v_2\left(\binom{n}{m}\right) = s_2(n-m) + s_2(m) - s_2(n).$$

   If we take $m = 2^i - 1$, then $n - m = \overline{a_{i-1} a_{i-2} \cdots a_1 1}$, so $s_2(n-m) + s_2(m) - s_2(n) = i + (s_2(n) + 1 - a_i) - s_2(n) = i$. Hence $i = \lfloor \log_2 n \rfloor$ satisfies $2^i \mid \binom{n}{m}$.

   There are a few ways to show optimality. We present three different solutions.

Solution 1: Basic NT. Let $d = \lfloor \log_2 n \rfloor$. Notice that

$$\lfloor x \rfloor + \lfloor y \rfloor + 1 \geq \lfloor x + y \rfloor$$

for any real x, y, hence

$$v_2\left(\frac{n!}{m!(n-m)!}\right) = \sum_{k=1}^{d} \left\lfloor \frac{n}{2^k} \right\rfloor - \left\lfloor \frac{n-m}{2^k} \right\rfloor - \left\lfloor \frac{m}{2^k} \right\rfloor \leq \sum_{k=1}^{d} 1 = d.$$

Solution 2: Digit Sum. We will show:

Lemma 1. *If m, n are arbitrary non-negative integers, then $s_2(m) + s_2(n) + 1 \leq s_2(m+n+1) + \log_2(m+n+1)$.*

Proof. By induction on $m+n$. Base case $m+n=0$ is trivial. For the inductive step, we casework on parity of m, n. For the following we will use the facts $s_2(x+1) \leq s_2(x) + 1$ and $s_2(2x+1) = s_2(2x) = s_2(x)$ for any non-negative integer x.

- If $m = 2a, n = 2b$ are both even, then $s_2(2a) + s_2(2b) + 1 = s_2(a) + s_2(b) + 1 \leq s_2(a+b+1) + \log_2(a+b+1) \leq s_2(a+b) + \log_2(a+b+1) + 1 \leq s_2(2a+2b+1) + \log_2(2a+2b+1)$.
- If $m = 2a+1, n = 2b+1$ are both odd, then $s_2(2a+1) + s_2(2b+1) + 1 = s_2(a) + s_2(b) + 3 \leq s_2(a+b+1) + \log_2(a+b+1) + 2 \leq s_2(2a+2b+3) + \log_2(2a+2b+3)$.
- If m, n are different parities, without loss of generality let $m = 2a$, $n = 2b+1$. Then $s_2(2a+1) + s_2(2b) + 1 = s_2(a) + s_2(b) + 2 \leq s_2(a+b+1) + \log_2(a+b+1) + 1 = s_2(2a+2b+2) + \log_2(2a+2b+2)$.

This completes the inductive step. □

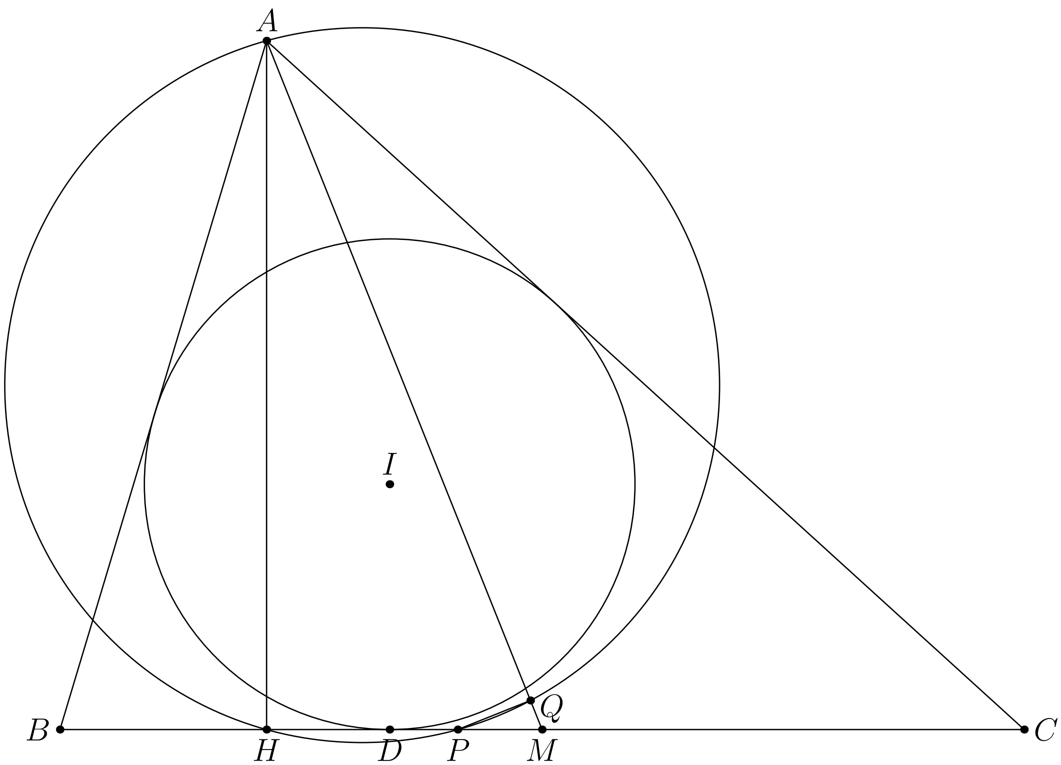
Since $s_2(n) + 1 \geq s_2(n+1)$, we obtain $s_2(m) + s_2(n) \leq s_2(m+n) + \log_2(m+n)$ for all $m \geq 0, n \geq 1$. Now one of $m, n-m$ is nonzero, hence $s_2(n) - s_2(m) - s_2(n-m) \leq \log_2 n$, proving the upper bound.

Solution 3: Base Carry. We claim $s_2(n) - s_2(m) - s_2(n-m)$ is the number of carries when adding m and $n-m$ in base 2. This is intuitively clear because a carry subtracts 2 from the current digit and adds 1 to the next digit, e.g. 13_2 becomes 21_2 (which then becomes 101_2 after another carry). Thus the number of carries is the number of 1s annihilated, which is just $s_2(n) - s_2(m) - s_2(n-m)$. Now if n has k digits, then carries can only happen in the 1st through $(k-1)$-th spots. Hence there are at most $k - 1 \leq \lfloor \log_2 n \rfloor$ carries.

Remark 1. Solution 2 is just a way to formalize the base carry in Solution 3 without actually carrying out the base carry. Some people will like it; others will complain of using a hammer to swat a fly.

3. Let ABC be a scalene triangle. The incircle of ABC touches $\overline{BC}$ at D. Let P be a point on $\overline{BC}$ satisfying $\angle BAP = \angle CAP$, and M be the midpoint of $\overline{BC}$. Define Q to be on $\overline{AM}$ such that $\overline{PQ} \perp \overline{AM}$. Prove that the circumcircle of $\triangle AQD$ is tangent to $\overline{BC}$.

   Proposed by: Ankan Bhattacharya.



Let H be the foot of the A-altitude. Then $AHPQ$ is cyclic, so $MQ \cdot MA = MP \cdot MH$. Let the side lengths of ABC be a, b, c, and let $s = \frac{a+b+c}{2}$. We can compute the following directed lengths:

$$\begin{aligned} MP &= \frac{ac}{b+c} - \frac{a}{2} = \frac{a(c-b)}{2(b+c)}, \\ MH &= c \cdot \frac{c^2+a^2-b^2}{2ac} - \frac{a}{2} = \frac{c^2-b^2}{2a}, \\ MD &= (s-b) - \frac{a}{2} = \frac{c-b}{2}. \end{aligned}$$

Thus, $MP \cdot MH = MD^2$, which means $MQ \cdot MA = MD^2$. The converse of Power of a Point shows the circumcircle of AQD is tangent to BC, as desired.

4. Find all functions $f : \mathbb{R} \to \mathbb{R}$ such that for all $x, y \in \mathbb{R}$,

$$f(f(x)+y)^2 = (x-y)(f(x)-f(y)) + 4f(x)f(y).$$

Proposed by: Kevin Ren.

Answer: $\boxed{f(x) = x + k \text{ for } k \in \mathbb{R} \text{ and } f(x) = 0}$.

Lemma 1. *Either $f(x) = 0$ or $f(x)$ is injective.*

Proof. Suppose $f(a) = f(b)$ for some $a \neq b \in \mathbb{R}$. Then $f(f(a)+y)^2 = (a-y)(f(a)-f(y)) + 4f(a)f(y)$ and $f(f(b)+y)^2 = (b-y)(f(b)-f(y)) + 4f(b)f(y)$. Thus $(a-y)(f(a)-f(y)) = (b-y)(f(a)-f(y))$. If $f(y) \neq f(a)$ for some y then $a - y = b - y$, which implies $a = b$, contradiction. Otherwise $f(y) = f(a)$ for all y implies f is constant. In this case, let $f(x) = C$. The condition gives $C^2 = 4C^2$, so $C = 0$. $\square$

Since $f(x) = 0$ is a solution, we restrict ourselves to the case where f is injective.

Lemma 2. $f(-f(0)) = 0$.

Proof. Let $x = 0$ and $y = -f(0)$. Then

$$f(0)^2 = f(0)(f(0) - f(-f(0))) + 4f(0)f(-f(0)) = f(0)^2 + 3f(0)f(-f(0)),$$

so $3f(0)f(-f(0)) = 0$. Thus $f(0) = 0$ or $f(-f(0)) = 0$. In either case $f(-f(0)) = 0$. □

Let $a = f(0)$; then $f(-a) = 0$. Now let $x = -a$. Then $f(y)^2 = (-a - y)(-f(y)) = (a + y)f(y)$. This implies $f(y) = 0$ or $f(y) = y + a$. Since f is injective, $f(y) \neq 0$ whenever $y \neq -a$. So, for $y \neq -a$, we have $f(y) = y + a$, and for $y = -a$ we have $f(y) = 0 = -a + a$. Thus $f(y) = y + a$ for all a, and this is a solution to the functional equation.

5. The number 2019 is written on a blackboard. Every minute, if the number a is written on the board, Evan erases it and replaces it with a number chosen from the set

$$\{0, 1, 2, \ldots, \lceil 2.01a \rceil\}$$

uniformly at random. Is there an integer N such that the board reads 0 after N steps with at least 99% probability?

Proposed by: Brice Huang and Ryan Alweiss.

Answer: $\boxed{\text{Yes}}$.

Throughout this solution we consider the random variable a_n denoting the number written after the nth minute; we extend the process infinitely by dictating that $a_{n+1} = 0$ if $a_n = 0$. We will show that

$$\mathbb{P}[a_n \neq 0] = O(c^n)$$

for some constant $c < 1$. This will imply the result.

Let m be a very large absolute constant. We begin by proving the following lemma.

Lemma 1. *If m is sufficiently large then,*

$$\mathbb{E}[\sqrt[m]{a_{n+1}}|a_n] \leq c\sqrt[m]{a_n}$$

for some constant $c < 1$ depending only on m.

Proof. First, assume $0 < a_n < 3$. Assume also that $\frac{9}{10} < c < 1$.

If $a_n = 1$, $\mathbb{E}[\sqrt[m]{a_{n+1}}|a_n] = \frac{\sqrt[m]{0} + \sqrt[m]{1} + \sqrt[m]{2} + \sqrt[m]{3}}{4} < \frac{3}{4}\sqrt[m]{3} < \frac{9}{10}\sqrt[m]{1}$ if m is large enough.

If $a_n = 2$, $\mathbb{E}[\sqrt[m]{a_{n+1}}|a_n] = \frac{\sqrt[m]{0} + \sqrt[m]{1} + \ldots + \sqrt[m]{5}}{6} < \frac{5}{6}\sqrt[m]{5} < \frac{9}{10}\sqrt[m]{2}$ if m is large enough.

If $a_n = 0$ there is nothing to prove. Now suppose $a_n \geq 3$; then

$$\begin{aligned}
\mathbb{E}[\sqrt[m]{a_{n+1}}|a_n] &= \frac{1}{\lceil 2.01a_n \rceil + 1}\left(\sum_{a=0}^{\lceil 2.01a_n \rceil} \sqrt[m]{a}\right) \\
&\leq \frac{1}{\lceil 2.01a_n \rceil + 1}\int_1^{\lceil 2.01a_n \rceil + 1} x^{\frac{1}{m}}\, dx \\
&\leq \frac{1}{\lceil 2.01a_n \rceil + 1} \cdot \frac{m}{m+1} \cdot \left[(\lceil 2.01a_n \rceil + 1)^{1+1/m} - 1\right] \\
&< \frac{m}{m+1}\,(2.01a_n + 2)^{1/m}.
\end{aligned}$$

Thus, we have

$$\frac{\mathbb{E}[\sqrt[m]{a_{n+1}}|a_n]}{\sqrt[m]{a_n}} < \frac{m}{m+1} \cdot \sqrt[m]{\frac{2.01a_n + 2}{a_n}} \leq \frac{m}{m+1} \cdot \sqrt[m]{2.01 + \frac{2}{3}}.$$

Since $2.01 + 2/3 < e = \lim_m (1 + 1/m)^m$, we can set $c = \frac{m}{m+1} \cdot \sqrt[m]{2.01 + \frac{2}{3}} < 1$ for m sufficiently large, as desired. □

Taking the expectation of both sides of the above lemma gives

$$\begin{aligned}
&\mathbb{E}[\mathbb{E}[\sqrt[m]{a_{n+1}}|a_n]] \leq \mathbb{E}[c\sqrt[m]{a_n}] \\
\implies &\mathbb{E}[\sqrt[m]{a_{n+1}}] \leq c \cdot \mathbb{E}[\sqrt[m]{a_n}].
\end{aligned}$$

So, by induction, we obtain

$$\mathbb{E}[\sqrt[m]{a_n}] \leq c^n \cdot \sqrt[m]{2019}.$$

But $\mathbb{E}[\sqrt[m]{a_n}] \geq \mathbb{P}[a_n \neq 0]$ which implies the result.

6. A *mirrored polynomial* is a polynomial f of degree 100 with real coefficients such that the x^{50} coefficient of f is 1, and $f(x) = x^{100} f(1/x)$ holds for all real nonzero x. Find the smallest real constant C such that any mirrored polynomial f satisfying $f(1) \geq C$ has a complex root z obeying $|z| = 1$.

Proposed by: Kevin Ren.

Answer: $\boxed{51}$.

Let $n = 100$, and let $f(x) = a_0 + a_1 x + \cdots + a_{2n} x^{2n}$ with $a_k = a_{2n-k}$. Define

$$g(\theta) = \frac{f(e^{i\theta})}{(e^{i\theta})^n} - 1 = a_{n-1} \cdot 2\cos\theta + a_{n-2} \cdot 2\cos 2\theta + \ldots + a_0 \cdot 2\cos n\theta.$$

Thus $e^{i\theta}$ is a root of f exactly when $g(\theta) = -1$.

Claim 1. *If $f(1) \geq 51$, then we can choose θ such that $g(\theta) = -1$.*

Proof. A roots of unity argument across the 51st roots of unity gives that

$$0 = g(0) + \sum_{k=1}^{50} g\left(\frac{2\pi k}{51}\right)$$

and so by pigeonhole there is some θ (of the form $\frac{2\pi k}{51}$) such that

$$g(\theta) \leq -\frac{g(0)}{50} = -\frac{f(1)-1}{50} \leq -1.$$

As $g(0) > -1$, by intermediate value theorem the conclusion follows. ☐

In the converse direction,

Claim 2. *There exist mirrored polynomials f with $f(1)$ arbitrarily close to 51 such that $g(\theta) > -1$ for each θ.*

Proof. Choose any real number $\lambda < 1$. Consider the choice

$$f(x) = 1 + \frac{\lambda}{51}(1 + 2x + 3x^2 + \cdots + 49x^{49}) + \frac{\lambda}{51}(x^{100} + 2x^{99} + 3x^{98} + \cdots + 49x^{51}).$$

As promised,

$$f(0) = 1 + \frac{2\lambda}{51}(1 + 2 + \cdots + 50) = 1 + 50\lambda$$

which is arbitrarily close to 51. And the corresponding g satisfies

$$\begin{aligned}
g(\theta) &= \frac{2\lambda}{51}\left(\cos 50\theta + 2\cos 49\theta + \cdots + 50\cos\theta\right) \\
&= \frac{2\lambda}{51}\sum_{j=1}^{50}\sum_{k=1}^{j}\cos k\theta \\
&= \frac{2\lambda}{51}\sum_{j=1}^{50}\frac{\sin(n+\frac{1}{2})\theta - \sin\frac{\theta}{2}}{2\sin\frac{\theta}{2}} \\
&= \frac{2\lambda}{51}\left(\frac{1-\cos 51\theta}{4\sin^2\frac{\theta}{2}} - \frac{51}{2}\right) \\
&= \frac{\lambda}{51}\left[\frac{1-\cos 51\theta}{1-\cos\theta} - 51\right] \ge -\lambda > -1
\end{aligned}$$

for all θ, ergo f has no roots on the unit circle. $\square$

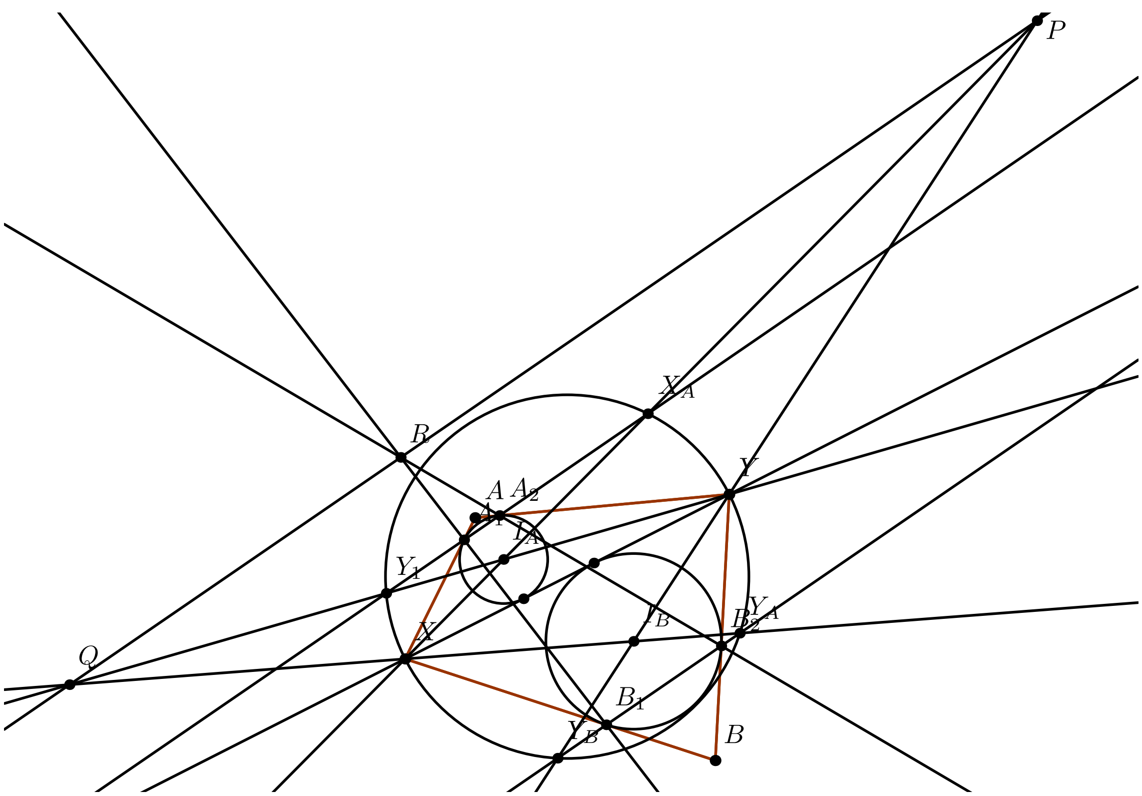
7. Let $AXBY$ be a convex quadrilateral. The incircle of $\triangle AXY$ has center I_A and touches $\overline{AX}$ and $\overline{AY}$ at A_1 and A_2 respectively. The incircle of $\triangle BXY$ has center I_B and touches $\overline{BX}$ and $\overline{BY}$ at B_1 and B_2 respectively. Define $P = \overline{XI_A} \cap \overline{YI_B}$, $Q = \overline{XI_B} \cap \overline{YI_A}$, and $R = \overline{A_1B_1} \cap \overline{A_2B_2}$.

   a. Prove that if $\angle AXB = \angle AYB$, then P, Q, R are collinear.

   b. Prove that if there exists a circle tangent to all four sides of $AXBY$, then P, Q, R are collinear.

Proposed by: Ankan Bhattacharya. Solution by Kevin Ren.

Solution to part (a).



Let ω be the circle with diameter XY. Let YI_A intersect ω at Y_A and XI_A intersect ω at X_A. Define Y_B, X_B similarly. By the Iran Incenter Lemma, Y_A, A_1, A_2, X_A are collinear and Y_B, B_1, B_2, X_B are collinear. By Pascal's theorem on $X_AXX_BY_BYY_A$, we have that X_AY_A, X_BY_B, and PQ are concurrent. But an easy angle chase shows $AI_A \parallel BI_B$, hence $A_1A_2 \parallel B_1B_2$, and so all three lines are actually parallel.

Now we will show $QR \parallel A_1A_2$; the claim that $PR \parallel A_1A_2$ will follow similarly. Let $d(L, \ell)$ be the distance from L to ℓ; it suffices to show that

$$\frac{d(Q, A_1A_2)}{d(Q, B_1B_2)} = \frac{d(R, A_1A_2)}{d(R, B_1B_2)}. \qquad (\star)$$

The last quantity equals $\frac{A_1A_2}{B_1B_2}$ by similar triangles; the first quantity equals

$$\frac{QY_A \sin\angle X_AY_AY}{QX_B \sin\angle XX_BY_B} = \frac{Y_AX \sin\angle I_AXY}{X_BY \sin\angle I_BYX} = \frac{\sin\angle I_AYX \sin\angle I_AXY}{\sin\angle I_BYX \sin\angle I_BXY}.$$

Recall the fact that in a triangle ABC, we have $r = 4R\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2}$. Now let r be the inradius and R be the circumradius of AXY; then

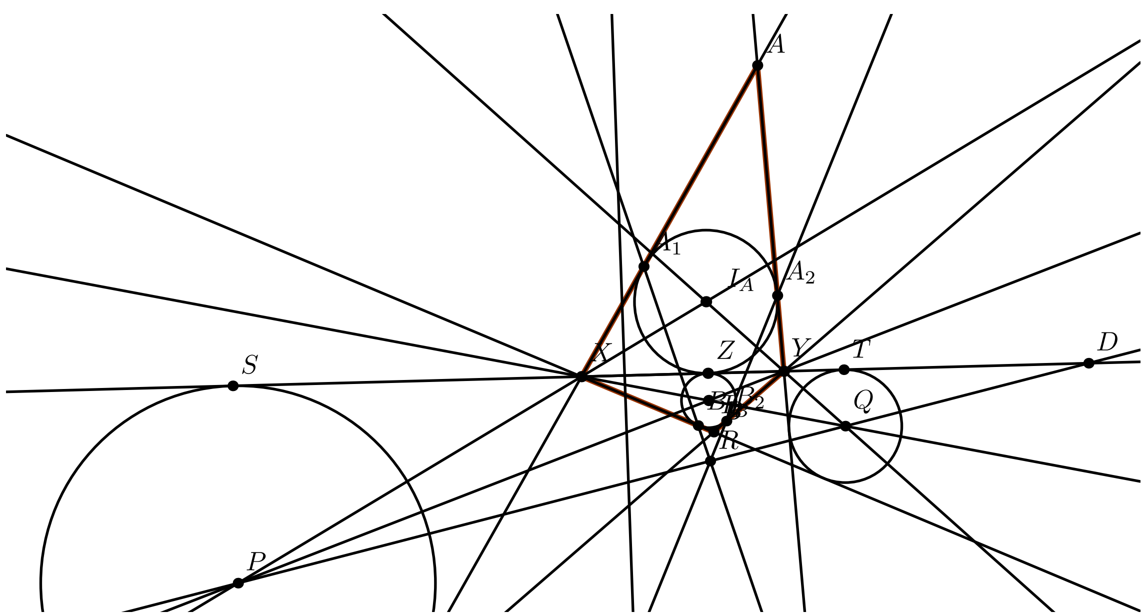
$$\frac{A_1A_2}{XY} = \frac{2r\cos\frac{A}{2}}{2R\sin A} = \frac{r}{2R\sin\frac{A}{2}} = 2\sin\frac{\angle AXY}{2}\sin\frac{\angle AYX}{2}$$

and similarly

$$\frac{B_1B_2}{XY} = 2\sin\frac{\angle BXY}{2}\sin\frac{\angle BYX}{2}.$$

Hence, $\frac{\sin\angle I_AYX \sin\angle I_AXY}{\sin\angle I_BYX \sin\angle I_BXY} = \frac{A_1A_2/(2XY)}{B_1B_2/(2XY)} = \frac{A_1A_2}{B_1B_2}$, showing that $(\star)$ is true. Thus, $PR \parallel A_1A_2$ and $QR \parallel A_1A_2$, which means P, Q, R are collinear, as desired.

Solution to part (b).



First, the incircles ω_A of AXY and ω_B of BXY meet XY at the same point Z. Next, $XA_1 = XZ = XB_1$ by equal tangents, so $\angle XA_1B_1 = \angle XB_1A_1$. This implies $\angle I_BB_1A_1 = \angle I_AA_1B_1$. Let A_1B_1 intersect ω_A again at A_3; then $\angle I_AA_3A_1 = \angle I_AA_1B_1 = \angle I_BB_1A_1$, so $I_AA_3 \parallel I_BB_1$. Hence, A_3 and B_1 are corresponding points on ω_A and ω_B, so A_3B_1 passes through the external center of homothety H' between ω_A and ω_B. Thus A_1B_1 passes through H'. Similarly A_2B_2 passes through H', so $R = H'$. There are multiple ways to finish from here.

Finish 1: Projective Geometry. Let I_AI_B meet PQ at R'. We aim to show $R' = R$.

Let PQ intersect XY at D. Because PY, QX, I_AR' are concurrent at I_B and XY meets PQ at D, we have by a well-known projective lemma that $(P, Q; R, D) = -1$. Projecting through X onto I_AI_B gives $(I_A, I_B; R', Z) = -1$. Since Z is the internal center of homothety between ω_A and ω_B, R must be the external center of homothety. This means $R = R'$, so P, Q, R are collinear.

Finish 2: Length Bash. We can show by computation that R is on I_1I_2 with $RZ = \frac{2r_1r_2}{r_1-r_2}$, where we use directed lengths with $ZI_A = r_1$ and $I_BZ = r_2$.

Now P is the center of a circle ω_P tangent to the extension of YX past X, the extension of YB past B, and the extension of AX past X. Let ω_P have radius r_3 and be tangent to XY at S, and define $SX = s, XZ = z, ZY = y$. Then a homothety at X relates ω_A and ω_P, and a homothety at Y relates ω_B and ω_P. Hence, $\frac{x}{s} = \frac{r_1}{r_3}$ and $\frac{y}{y+x+s} = \frac{r_2}{r_3}$. Solving, we get $s = \frac{r_2x(x+y)}{r_1y-r_2x}$, so $x + s = \frac{(r_1+r_2)xy}{r_1y-r_2x}$. Also $r_3 = \frac{r_1s}{x} = \frac{r_1r_2(x+y)}{r_1y-r_2x}$, so $\frac{x+s}{r_3} = \frac{(r_1+r_2)xy}{r_1r_2(x+y)}$. Similarly define ω_Q with radius r_4 and tangent to XY at T, and $YT = t$; then $t = \frac{r_2y(x+y)}{r_1x-r_2y}$, $y + t = \frac{(r_1+r_2)xy}{r_1x-r_2y}$, $r_4 = \frac{r_1r_2(x+y)}{r_1x-r_2y}$, and $\frac{y+t}{r_4} = \frac{(r_1+r_2)xy}{r_1r_2(x+y)} = \frac{x+s}{r_3}$. Let U be the internal center of homothety between ω_P and ω_Q, and V be the projection of U onto XY. Then we can easily see $\frac{SV}{VT} = \frac{r_3}{r_4} = \frac{SZ}{ZT}$, so $V = Z$. Furthermore, we can compute

$$UV = r_3 \cdot \frac{y+t}{x+y+s+t} + r_4 \cdot \frac{x+s}{x+y+s+t}$$

$$= r_3 \cdot \frac{r_1y - r_2x}{(r_1-r_2)(x+y)} + r_4 \cdot \frac{r_1x - r_2y}{(r_1-r_2)(x+y)} = \frac{2r_1r_2}{r_1-r_2} = RZ,$$

so $R = U$. Hence, P, Q, R are collinear.

Remark 1. Some teams claimed that P, Q, R are always collinear by a Desargues' theorem argument. Actually this proves that A_1A_2, B_1B_2, and PQ are either all concurrent or all parallel.

8. Find all pairs of positive integers (m, n) such that $(2^m - 1)(2^n - 1)$ is a perfect square.

   Proposed by: Kevin Ren.

   Answer: $\boxed{(3,6),\ (6,3),\ (m,m) \text{ for } m \in \mathbb{N}}$.

   Let $v_p(n)$ be the exponent of p in the prime factorization of n. We will cite without proof several well-known facts:

   Lemma 1 (LTE). *If p is an odd prime that divides $a - b$, then $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$.*

   Corollary 2 (CLTE). *If p is an odd prime, $p \mid a^n - 1$, and $p \mid \frac{a^{mn}-1}{a^n-1}$ for some integers a, m, n, then $p \mid m$.*

   Lemma 3. *For any integers m, n, we have $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m,n)} - 1$.*

   Lemma 4. *If a, b are positive integers with $\gcd(a, b) = 1$ and ab is a perfect square, then a and b are perfect squares.*

   We will prove:

   Theorem 5. *If m, n are positive integers, then $\frac{2^{mn}-1}{2^m-1}$ is a perfect square only if either $n = 1$, or $m = 3$ and $n = 2$.*

   Lemma 6. *If $2^k + 1$ is a perfect square, then $k = 3$.*

   Proof. We have $2^k + 1 = x^2$ for some integer x, so $2^k = (x - 1)(x + 1)$. Thus both $x - 1$ and $x + 1$ are powers of 2, which means $x = 3$. Then $k = 3$. ☐

   Proposition 7. *If n is even, then $n = 2$ and $m = 3$.*

Proof. Let $n = 2k$ for some k. Write

$$\frac{2^{2mk}-1}{2^m-1} = (2^{mk}+1) \cdot \frac{2^{mk}-1}{2^m-1}.$$

Since $2^{mk}+1$ and $2^{mk}-1$ are relatively prime, we have $2^{mk}+1$ and $\frac{2^{mk}-1}{2^m-1}$ are relatively prime. Because they multiply to a perfect square, they are both perfect squares by Lemma 4. By Lemma 6, we must have $mk = 3$, so $k = 3$ and $m = 1$, or $m = 3$ and $k = 1$. Only the second case makes $\frac{2^{2mk}-1}{2^m-1}$ a perfect square, so $m = 3$ and $n = 2$. $\square$

Therefore, we may assume that n is odd. Now we need an algebraic lemma:

Lemma 8. *If n is odd, then $m \le n-2$.*

Proof. Recall the power series

$$\frac{1}{\sqrt{1-x}} = \sum_{n=0}^{\infty} c_n x^n$$

where $c_n = \frac{\binom{2n}{n}}{4^n}$. Squaring the series, we have $\sum_{k=0}^{n} c_k c_{n-k} = 1$ for all n. Now define $r = \frac{n-1}{2}$ and

$$P(x) = \sum_{k=1}^{r} x^k c_{r-k}.$$

Then

$$P(x)^2 = \sum_{j=1}^{r}\sum_{k=1}^{r} x^{j+k} c_{r-j} c_{r-k} = \sum_{k=0}^{2r} x^{2r-k} \sum_{a+b=k, 0\le a,b\le r-1} c_a c_b < \sum_{k=0}^{2r} x^k$$

and

$$(P(x)+1)^2 \ge \sum_{k=r+1}^{2r} x^k + 2x^r > \sum_{k=0}^{2r} x^k$$

whenever $x \ge 2$, since $\sum_{k=0}^{r-1} x^k = \frac{x^r-1}{x-1} < x^r$. If $m > n-2$, then $P(2^m)$ is an integer, and so $\frac{x^n-1}{x-1} = \sum_{k=0}^{2r} x^k$ would be between two perfect squares. This implies $\frac{2^{mn}-1}{2^m-1}$ is not a perfect square, contradiction. Hence, in fact $m \le n-2$. $\square$

We will also need the following smaller lemmas.

Lemma 9. *If $2^k - 1$ is a perfect square for some $k \ge 1$, then $k = 1$.*

Proof. If $k \ge 2$ then $2^k - 1 \equiv 3 \pmod 4$ can never be a perfect square. $\square$

Lemma 10. *Call a positive integer k p-suitable if all prime factors of k are greater than p. If p is prime and k is p-suitable, then $p \nmid 2^k - 1$.*

Proof. Trivial if $p = 2$. If $p \ge 3$ then we have $p \mid 2^{p-1} - 1$. If $p \mid 2^k - 1$ then $p \mid 2^{\gcd(p-1,k)} - 1 = 1$, contradiction. $\square$

Proposition 11. $\frac{2^{p^a kr}-1}{2^{p^b k}-1}$ *cannot be a perfect square for any odd prime p and integers $a > b \ge 0$, and p-suitable integers k, r.*

Proof. If $a = k = r = 1$ then $b = 0$ and our expression becomes $2^p - 1$, which is not a perfect square by Lemma 9. Suppose not all of a, k, r are one; then $p^{a-1}kr \ne 1$ and has all prime factors at least p, so $p^{a-1}kr \ge p$. We have $\frac{2^{p^a kr}-1}{2^{p^b k}-1} = \frac{2^{p^{a-1}kr}-1}{2^{p^b k}-1} \cdot \frac{2^{p^a kr}-1}{2^{p^{a-1}kr}-1}$. Since k, r are p-suitable, by Lemma 10, $p \nmid 2^{p^{a-1}kr} - 1$. Hence, any prime divisor of the first term can't divide the second term by CLTE. Thus, the two terms are relatively prime. However, the second term is not a perfect square by Lemma 8 and $p^{a-1}kr \ge p$, so by Lemma 4, $\frac{2^{p^a kr}-1}{2^{p^b k}-1}$ is not a perfect square. $\square$

Proposition 12. *If $\frac{2^{p^a kr}-1}{2^{p^a k}-1}$ is a perfect square for some prime p and integers $a \geq 0$, and p-suitable integers k, r, then so is $\frac{2^{kr}-1}{2^k-1}$.*

Proof. Write

$$\frac{2^{p^a kr}-1}{2^{p^a k}-1} = \frac{2^{kr}-1}{2^k-1} \cdot \frac{(2^{p^a kr}-1)(2^k-1)}{(2^{p^a k}-1)(2^{kr}-1)}.$$

We will verify that the second term on the RHS is an integer. Since $2^{p^a k}-1$ and $2^{kr}-1$ both divide $2^{p^a kr}-1$, it suffices to verify that $v_q(2^{p^a k}-1)+v_q(2^{kr}-1) \leq v_q(2^{p^a kr}-1)+v_q(2^k-1)$ whenever $q \mid 2^{p^a k}-1$ and $q \mid 2^{kr}-1$. By Lemma 3, we have $q \mid 2^k-1$. Then the inequality is actually an equality by LTE.

Now we claim the two terms on the RHS are relatively prime. If $q \mid \frac{2^{kr}-1}{2^k-1}$ then $q \mid 2^{kr}-1$. Now if $q \mid 2^k-1$ then $q \nmid \frac{(2^{p^a kr}-1)(2^k-1)}{(2^{p^a k}-1)(2^{kr}-1)}$ by LTE, and if $q \nmid 2^k-1$, then $q \neq p$ by Lemma 10. Thus by CLTE, $q \nmid \frac{2^{p^a kr}-1}{2^{kr}-1}$. Hence, in either case the two terms on the RHS are relatively prime, which means they are perfect squares by Lemma 4. In particular, the first term is a perfect square. $\square$

Finally, we prove our main result.

Proof of Theorem 5. We induct on the number of prime factors of m. If $m=1$ then $n=1$ by Lemma 9. Suppose $m>1$ and let p be the least prime factor of m. If $v_p(n)=0$ then apply Proposition 12 to reduce to the case $\left(\frac{m}{p^{v_p(m)}}, n\right)$. If $v_p(n)>0$ then $p \neq 2$ (since n is odd), so there are no solutions by Proposition 11. This completes the inductive step and thus the proof.

Now we are ready to solve the problem. The answer is $(3,6),(6,3),(m,m)$. Verify that $(2^3-1)(2^6-1) = 7 \cdot 63 = 21^2$.

To see that no other (m,n) work, let $d=\gcd(m,n)$. Without loss of generality, let $m<n$. Then $\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}-1$, so for $(2^m-1)(2^n-1)$ to be a perfect square, we must have $\frac{2^m-1}{2^d-1}$ and $\frac{2^n-1}{2^d-1}$ be perfect squares as well. Because $m<n$, we have $n>d$. By Theorem 5, we have $d=3$ and $n=6$. This forces $m=3$. $\square$