Solutions to the year 2000 International Mathematical Olympiad*

Ilan Vardi†

This article is meant to complement my earlier paper on Mekh–mat entrance examinations [9]. In that paper I stated that the Mekh–mat problems appeared to be at the level of Olympiad problems which were an appropriate standard for comparison. In order to verify this claim, I decided to solve under similar conditions (without use of outside references or help) all the problems for a given Olympiad year. Doing *all* problems in a given year appears to be the fairest test of problem solving, as one cannot simply choose the problems one is best at. Finally, since many people work on Olympiad problems, one can compare one's solution with the best that has been found (this was not always possible with the Mekh–mat problems).

My conclusion is that the IMO problems are generally much more challenging than the Mekh–mat problems. In particular, it took me about 6 weeks to complete all the Olympiad problems and 6 weeks for all the Mekh–mat problems. However, there were 6 Olympiad problems versus 25 Mekh–mat problems.

On the other hand, the Olympiad problems were in general less interesting than the Mekh–mat problems. In fact, I only found Olympiad problems **3** and **6** to be interesting. Problem **3** required an interesting idea which took me a long time to discover (3 weeks!), and it also took me a long time to find an idea for **6**, which follows from a result of some independent interest (Lemma 6.3).

The other problems were solved in a relatively short time without too much difficulty. If there was an idea in **2** then I missed it as my solution consists of a completely unmotivated algebraic manipulation. Problem 5 is stated confusingly and has an alternate, possibly intractable interpretation. The lack of clarity might have been intentional in order not to give away the solution, see Remark 5.1.

The statements of the geometry questions **1** and **6** are of Byzantine complexity, and this appears to be typical of the geometry questions posed in the IMO. Moreover, Problem **1** is in some sense deceptive. In comparison, the Mekh–mat geometry problems were very elegant and in general interesting. Mekh–mat problems **1** and **2** were of comparable difficulty to the geometry problems posed here.

Since the source of the Mekh–mat problems [8] only included one number theory question and one combinatorial question, it is less meaningful to compare the other problems to the Mekh–mat questions.

I would like to thank K.S. Sarkaria and Harry Tamvakis for helpful comments. Alternate solutions appear on John Scholes' IMO web site [7]. Further IMO problems are given in [1] [3] [5] [6].

*41st IMO, Taejon, South Korea. International Mathematical Olympiad site: `olympiads.win.tue.nl/imo/`

†Preliminary version, November 2000. IHES, 35 route de Chartres, 91440 Bures–sur–Yvette, ilan@ihes.fr

1 Problems

Day 1

1. Two circles Γ_1 and Γ_2 intersect at M and N.

   Let ℓ be the common tangent to Γ_1 and Γ_2 so that M is closer to ℓ than N is. Let ℓ touch Γ_1 at A and Γ_2 at B. Let the line through M parallel to ℓ meet the circle Γ_1 again at C and the circle Γ_2 again at D.

   Lines CA and DB meet at E; lines AN and CD meet at P; lines BN and CD meet at Q.

   Show that $EP = EQ$.

2. Let a, b, c be positive real numbers such that $abc = 1$. Prove that

$$\left(a - 1 + \frac{1}{b}\right)\left(b - 1 + \frac{1}{c}\right)\left(c - 1 + \frac{1}{a}\right) \leq 1\,.$$

3. Let $n \geq 2$ be a positive integer. Initially, there are n fleas on a horizontal line, not all at the same point. For a positive real number λ, define a *move* as follows:

   choose any two fleas, at points A and B, with A to the left of B;

   let the flea at A jump to the point C on the line to the right of B with $BC/AB = \lambda$.

   Determine all values of λ such that, for any point M on the line and any initial positions of the n fleas, there is a finite sequence of moves that will take all the fleas to positions to the right of M.

Day 2

4. A magician has one hundred cards numbered 1 to 100. He puts them into three boxes, a red one, a white one and a blue one, so that each box contains at least one card.

   A member of the audience selects two of the three boxes, chooses one card from each and announces the sum of the numbers on the chosen cards. Given this sum, the magician identifies the box from which no card has been chosen.

   How many ways are there to put all the cards into boxes so that this trick always works? (Two ways are considered different if at least one card is put into a different box.)

5. Determine whether or not there exists a positive integer n such that n is divisible by exactly 2000 different prime numbers, and $2^n + 1$ is divisible by n.

6. Let AH_1, BH_2, CH_3 be the altitudes of an acute–angled triangle ABC. The incircle of the triangle ABC touches the sides BC, CA, AB at T_1, T_2, T_3, respectively. Let the lines ℓ_1, ℓ_2, ℓ_3 be the reflections of the lines H_2H_3, H_3H_1, H_1H_2 in the lines T_2T_3, T_3T_1, T_1T_2, respectively.

   Prove that ℓ_1, ℓ_2, ℓ_3 determine a triangle whose vertices lie on the incircle of the triangle ABC.

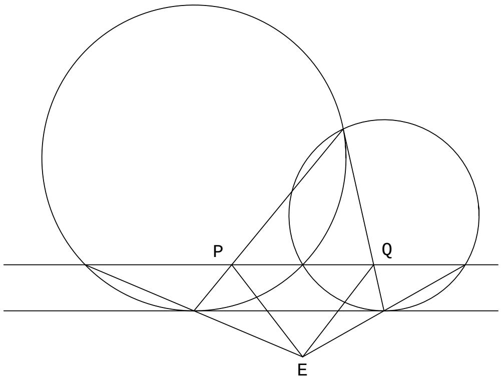
2 Solutions

Problem 1. *Two circles Γ_1 and Γ_2 intersect at M and N.*

Let ℓ be the common tangent to Γ_1 and Γ_2 so that M is closer to ℓ than N is. Let ℓ touch Γ_1 at A and Γ_2 at B. Let the line through M parallel to ℓ meet the circle Γ_1 again at C and the circle Γ_2 again at D.

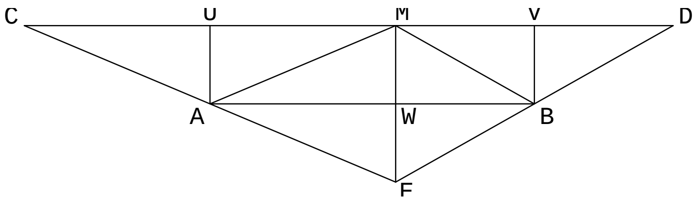
Lines CA and DB meet at E; lines AN and CD meet at P; lines BN and CD meet at Q.

Show that $EP = EQ$.



Solution: The somewhat complicated formulation of this problem is deceptive, and it is easily seen to be a combination of two simple results.

One starts by looking at a subproblem which can be analyzed by consideration of similar triangles, that is, the points A, B, C, D, E, M. In order to do this, one introduces 3 new points U, V, W, which are the midpoints of CM, MD and AB, respectively.



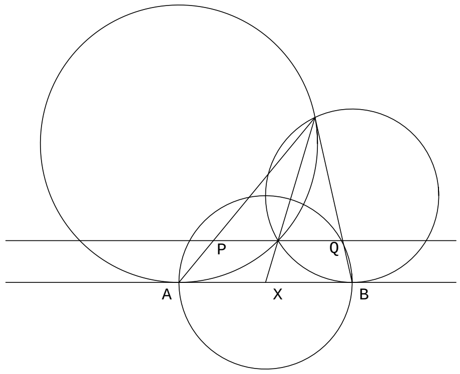
Since CM is a chord of the circle Γ_1 and A lies on Γ_1, it follows that $AC = AM$. Thus, $\angle MCA = \angle CMA$. Since CM is parallel to AB, $\angle CMA = \angle BAM$.

It follows $CU = UM = AW$. Similarly, one has $DV = VM = BW$. One therefore sees that $CD = 2CU + 2DV = 2AB$.

But, since CD and AB are parallel, the triangle CDA is similar to the triangle ABE, so it follows that $CE = 2\,AE$, in other words, that $CA = AE$. Finally, since $\angle BAE = \angle BAM$, one sees that EM is perpendicular to AB. The first result is therefore

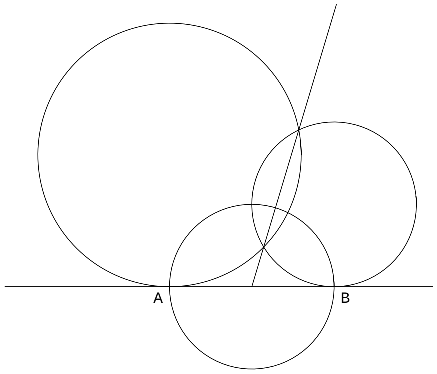
Lemma 1.1. *Under the assumptions of Problem 1, EM is perpendicular to AB.*

This result clarifies the situation considerably since it is now clear that $EP = EQ$ if and only if $MP = MQ$, since CD is also perpendicular to EM.



One therefore turns to the proof of $MP = MQ$. Extend the line MN to intersection AB at X. Since CD is parallel to AB, it follows that triangle NPM is similar to triangle NAX and that triangle NQM is similar to triangle NBX. The result therefore follows from the following interesting fact.

Lemma 1.2. *Let a line be tangent to two distinct circles at two different points A and B. Then the line joining the intersections of the two circles (or the tangent line if they touch once) bisects the line segment AB.*



Proof: The proof uses some elementary properties of inversion, see [2]. Let the notation be as in Problem 1, i.e., let Γ_1, Γ_2 be the circles, M and N be the intersection points and X the midpoint of AB.

Consider the circle Γ with center at X and radius AX. One does an inversion with respect to this circle. Since Γ_1 and Γ_2 are orthogonal to Γ (this is obvious at A and B), they are preserved. Since the line containing MN passes through infinity, it is transformed into a line or circle passing through X. However, since Γ_1 and Γ_2 are preserved, M is mapped to N and N is mapped to M. Finally, let the line MN intersect Γ at Y, then Y is fixed, since it lies on Γ. Thus, the line MN goes to a line or circle containing X, M, N, and Y. However, M, N, and Y lie on a line, therefore MN goes to a straight line, in particular to itself. One concludes that the line MN passes through X, which is the midpoint of AB and the result follows. The case in which the circle are tangent is left as an exercise.

Remark 1.1. Harry Tamvakis has noted that Lemma 3.2 follows easily using the *power of a point with respect to a circle.* In other words, it is easily shown that if the point X is external to a circle Γ, then for any line XMN touching the circle at M and N, then $XM \times MN$ is a constant (in the case in which the line XA is tangent to the circle, one takes $XA \times XA$).

Problem 2. *Let a, b, c be positive real numbers such that $abc = 1$. Prove that*

$$\left(a - 1 + \frac{1}{b}\right)\left(b - 1 + \frac{1}{c}\right)\left(c - 1 + \frac{1}{a}\right) \le 1\,.$$

Proof: The proof relies on the following identity.

Lemma 2.1. *Let a, b, c be positive real numbers such that $abc = 1$, then*

$$\begin{aligned} &1 - \left(a - 1 + \frac{1}{b}\right)\left(b - 1 + \frac{1}{c}\right)\left(c - 1 + \frac{1}{a}\right) \\ &\quad = \left(c + \frac{1}{c} - 2\right)\left(a + \frac{1}{b} - 1\right) + \left(1 - \frac{1}{a}\right)(1 - b)\,. \end{aligned} \tag{1}$$

This identity easily implies the result. To see this, note that if $abc = 1$, then at least one of a, b, c is ≥ 1 and at least one is ≤ 1. It follows that at least one of the ordered pairs (a, b), (b, c), or (c, a) has its first element ≥ 1 and the second ≤ 1. One can, without loss of generality, take this ordered pair to be (a, b). The reason is that Lemma 2.1 will be applied, and this result also holds with the variables on the right hand side of (1) replaced by $(a, b, c) \mapsto (c, a, b)$ and $(a, b, c) \mapsto (b, c, a)$, since the left hand side of (1) is invariant under these cyclic shifts.

One now applies Lemma 2.1. First one uses the arithmetic–geometric inequality which gives

$$\frac{1}{2}\left(c + \frac{1}{c}\right) \ge \sqrt{c \cdot \frac{1}{c}} = 1\,,$$

so that

$$c + \frac{1}{c} - 2 \ge 0.$$

Since $a \ge 1$ and $b \le 1$, one has

$$a + \frac{1}{b} - 1 \ge 0, \quad 1 - \frac{1}{a} \ge 0, \quad 1 - b \ge 0\,.$$

It follows that each term on the right hand side of (1) is non–negative which proves the result.

Proof of Lemma 2.1: One expands

$$\left(a - 1 + \frac{1}{b}\right)\left(b - 1 + \frac{1}{c}\right)\left(c - 1 + \frac{1}{a}\right)$$

using the transformation rules $ab \mapsto 1/c$, $ac \mapsto 1/b$, $bc \mapsto 1/a$. Thus

$$\begin{aligned} \left(b - 1 + \frac{1}{c}\right)\left(c - 1 + \frac{1}{a}\right) &= \frac{1}{a} - b + \frac{b}{a} - c + 1 - \frac{1}{a} + 1 - \frac{1}{c} + b \\ &= \frac{b}{a} + 2 - c - \frac{1}{c}\,. \end{aligned}$$

One continues with

$$\begin{aligned} \left(a - 1 + \frac{1}{b}\right)\left(\frac{b}{a} + 2 - c - \frac{1}{c}\right) &= b + 2a - \frac{1}{b} - \frac{a}{c} - \frac{b}{a} - 2 + c + \frac{1}{c} + \frac{1}{a} + \frac{2}{b} - \frac{c}{b} - a \\ &= a + \frac{1}{a} + b + \frac{1}{b} + c + \frac{1}{c} - \frac{a}{c} - \frac{c}{b} - \frac{b}{a} - 2\,. \end{aligned}$$

Thus, the left hand side of (1) equals

$$3+\frac{a}{c}+\frac{c}{b}+\frac{b}{a}-a-\frac{1}{a}-b-\frac{1}{b}-c-\frac{1}{c}\,. \tag{2}$$

One now computes

$$\begin{aligned}\left(c+\frac{1}{c}-2\right)\left(a+\frac{1}{b}-1\right) &= \frac{1}{b}+\frac{c}{b}-c+\frac{a}{c}+a-\frac{1}{c}-2a-\frac{2}{b}+2\\ &= 2+\frac{a}{c}+\frac{c}{b}-a-\frac{1}{b}-c-\frac{1}{c}\,,\end{aligned} \tag{3}$$

and

$$\left(1-\frac{1}{a}\right)(1-b)=1-b-\frac{1}{a}+\frac{b}{a}\,. \tag{4}$$

It is seen that the right hand sides of (3) and (4) add up to the right hand side of (3), which proves Lemma 2.1.

Remark 2.1. This proof appears to be completely unmotivated. In particular, there does not seem to be a conceptual explanation for the identity of Lemma 2.1. However, this identity fits into the general principle that inequalities should follow from identities, e.g., from the positivity of perfect squares [10].

Remark 2.2. A similar argument was found by Robin Chapman [7] using the identity

$$\left(a-1+\frac{1}{b}\right)\left(b-1+\frac{1}{c}\right)=b\left(a^2-\left(1-\frac{1}{b}\right)^2\right)\,.$$

This shows that the left hand side is $\le b\,a^2$, so the product of the three such identities is $\le b\,a^2\,c\,b^2\,ac^2=1$, which yields the square of the desired inequality. This works if all terms in the product are positive, but it is easily shown that at most one such term can be negative, in which case the inequality also holds.

Remark 2.3. One can try the general method of Lagrange multipliers to solve this problem. However, this method is usually considered beyond the scope of the High School curriculum.

Problem 3. *Let $n \ge 2$ be a positive integer. Initially, there are n fleas on a horizontal line, not all at the same point. For a positive real number λ, define a move as follows:*

> *choose any two fleas, at points A and B, with A to the left of B;*
>
> *let the flea at A jump to the point C on the line to the right of B with $BC/AB=\lambda$.*

Determine all values of λ such that, for any point M on the line and any initial positions of the n fleas, there is a finite sequence of moves that will take all the fleas to positions to the right of M.

Solution: All values $\lambda \ge 1/(n-1)$.

Proof: (a) First assume that $\lambda \ge 1/(n-1)$. Call a jump of (any) leftmost flea over the rightmost flea a *big move*. Then the fleas will all go to $+\infty$ using a succession of big moves.

First, assume that the fleas all at distinct positions, let $x_n < x_{n-1} < \cdots < x_1$ be the position of the fleas, and let m be the minimum distance between any two consecutive fleas.

One now performs a big move which puts the fleas at positions $x'_n < x'_{n-1} < \cdots < x'_1$, where $x_{n'} = x_{n-1}, \ldots, x'_2 = x_1$, and $x'_1 = x_1 + \lambda(x_1 - x_n)$.

Let m' be the minimum of the differences between consecutive fleas in the new position. Since $x'_n, \dots, x'_2$ are the same as in the previous position, it follows that the new minimum satisfies $m' \geq \min(m, x'_1 - x'_2)$. However, $x'_1 - x'_2 = \lambda (x_1 - x_n)$ and $x_1 - x_m \geq (n-1)\, m$. It follows that $m' \geq \min(m, \lambda(n-1)m) \geq m$, since $\lambda(n-1) \geq 1$, by assumption.

It follows that the minimum distance between consecutive fleas is nondecreasing. Thus, let $M > 0$ be a lower bound for all these minimum distance. It follows that $x'_n \geq x_n + M$, i.e., the rightmost flea moves at least distance M to the right at every iteration. This shows that all the fleas go to $+\infty$.

If the fleas are not all distinct, then, since at least two fleas are distinct, it is clear that after at most $n-1$ iterations of big moves, all fleas will become distinct, which reduces to the previous case.

(b) Assume that $\lambda < 1/(n-1)$. This seems to require some kind of physicial reasoning, as direct methods such as those in part (a) do not seem to work, see Remark 3.1.

Thus, one sees that there is a tradeoff between the position of the rightmost flea and the distance between the fleas. In other words, a greater distance to the right incurs a penalty in the distance between the fleas. Thus, one is led to the consideration of an *energy* to each placement of the fleas, where the position of the fleas is the *kinetic energy*, and the distances between the fleas is the *potential energy*.

By careful examination of the case of two fleas, one is led to the following definition.

Definition. Let the position of the fleas be $x = (x_1, x_2, \dots, x_n)$, where $x_1 \geq x_2 \geq \cdots \leq x_n$, then the *kinetic energy* $K(x)$ and the potential energy $P(x)$ are

$$K(x) = x_1, \qquad P_\alpha(x) = \alpha \sum_{i=2}^{n} (x_1 - x_i)\,,$$

where α is a constant. The *total energy* is $E_\alpha(x) = K(x) + P_\alpha(x)$.

This leads to the following.

Lemma 3.1. *If $\alpha = \lambda/(1-(n-1)\lambda)$, then the energy is never increased by a move.*

The main result follows directly from Lemma 3.1. Indeed, let $P(x) = P_{\lambda/(1-(n-1)\lambda)}(x)$. Since $\lambda < 1/(n-1)$, one has $\lambda/(1-(n-1)\lambda) > 0$ so that the potential energy is always positive. The Lemma shows that $K(x) + P(x) \leq E$ for some E independent of x, thus $K(x) \leq E - P(x) \leq E$ for all x, and the result follows.

Proof of Lemma 3.1: First consider the case of a big move. Thus, the fleas are initially at $x_n \leq \cdots \leq x_1$ and x_n jumps to $x'_1 = x_1 + \lambda(x_1 - x_n)$, while the other fleas remain at the same positions, i.e., $x'_n = x_{n-1}, \dots, x'_2 = x_1$.

The change in potential energy is

$$\begin{aligned} P_\alpha(x') - P_\alpha(x) &= \alpha \sum_{i=2}^{n} (x'_1 - x'_i) - \alpha \sum_{i=2}^{n} (x_1 - x_i) \\ &= \alpha \sum_{i=1}^{n-1} [(x'_1 - x_1) + (x_1 - x_i)] - \alpha \sum_{i=2}^{n} (x_1 - x_i) = (n-1)\, \alpha (x'_1 - x_1) - \alpha (x_1 - x_n) \\ &= \alpha[(n-1)\lambda - 1](x_1 - x_n)\,. \end{aligned}$$

Moreover, the change in kinetic energy is

$$K(x') - K(x) = x'_1 - x_1 = \lambda(x_1 - x_n)\,.$$

Thus, the difference in total energy is

$$
\begin{aligned}
E_\alpha(x') - E_\alpha(x) &= K(x') - K(x) + P_\alpha(x') - P_\alpha(x) = \lambda(x_1 - x_n) + \alpha[(n-1)\lambda - 1](x_1 - x_n) \\
&= (x_1 - x_n)(\lambda + \alpha[(n-1)\lambda - 1])\,,
\end{aligned}
$$

which is clearly zero when $\alpha = \lambda/(1-(n-1)\lambda)$. One has therefore proved

Lemma 3.2. *If $\alpha = \lambda/(1-(n-1)\lambda)$, then the total energy is preserved by a big move.*

One now considers other types of moves. The first possibility is if $x_1' = x_1$, i.e., the position of the rightmost flea does not change. In this case, the kinetic energy stays the same, while the potential energy decreases, for any $\alpha > 0$. This is obvious, since

$$
P_\alpha(x') - P_\alpha(x) = \alpha(x_i - x_j') < 0\,,
$$

where the move consisted of flea x_i jumping to x_j', and $x_j' > x_i$.

Finally, one considers the possibility that $x_1' > x_1$, but that this is not the result of a big move, i.e., the flea x_1' was previously at x_j, where $x_j > x_n$. One performs the same computation as with a big move. The change in potential energy is

$$
\begin{aligned}
P_\alpha(x') - P_\alpha(x) &= \alpha \sum_{i=2}^{n} (x_1' - x_i') - \alpha \sum_{i=2}^{n} (x_1 - x_i) \\
&= \alpha \sum_{\substack{1 \le i \le n \\ i \ne j}} [(x_1' - x_1) + (x_1 - x_i)] - \alpha \sum_{i=2}^{n} (x_1 - x_i) = (n-1)\,\alpha(x_1' - x_1) - \alpha(x_1 - x_j) \\
&\le \alpha[(n-1)\lambda - 1](x_1 - x_j)\,,
\end{aligned}
$$

since $x_1' - x_1 \le \lambda(x_1 - x_j)$, as x_j could at most jump over x_1. Similarly, the change in kinetic energy is

$$
K(x') - K(x) = x_1' - x_1 \le \lambda(x_1 - x_j)\,,
$$

so that the total change in energy is

$$
E(x') - E(x) \le (\lambda + \alpha[(n-1)\lambda - 1])(x_1 - x_j) = 0\,,
$$

if $\alpha = \lambda/(1-(n-1)\lambda)$. This shows that the total energy is nonincreasing, which finishes the proof of Lemma 3.1.

Remark 3.1. This type of solution was previously discovered by Gerhard Woeginger [7].

Remark 3.2. It can be shown directly that the strategy used in part (a), i.e, using only big moves, does not take the fleas to $+\infty$. In fact, a big move is a linear transformation $x' = Ax$, where A is the matrix

$$
A = \begin{pmatrix}
1+\lambda & 0 & \cdots & 0 & -\lambda \\
1 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0
\end{pmatrix}.
$$

This matrix has characteristic polynomial $(x-1)(x^{n-1}-\lambda(x^{n-2}+x^{n-3}+\cdots+1))$, which has one eigenvalue 1 while all other eigenvalues have absolute value strictly less than 1, when $\lambda < 1/(n-1)$.

Using this method, or equivalent methods, it is simple to show that $x_1 - x_n \to 0$ exponentially, i.e., the distance between the rightmost flea and the leftmost flea goes to zero exponentially. Since, in a simple iteration of big moves, the position of the rightmost flea is essentially the sum of these distances, one gets that the position of the rightmost flea is bounded above.

However, this argument seems to break down if other types of moves are allowed. In particular, the distance between the rightmost and lefmost fleas no longer has to go to zero, e.g., if the leftmost flea never moves. Moreover, for moves other than big moves, the relabelling of the fleas depends is no longer unique, as a flea may land between any two others, to that the choice of matrix is no longer unique. Finally, even without this problem, the asymptotics of random matrix products is a nontrivial question.

Problem 4. *A magician has one hundred cards numbered 1 to 100. He puts them into three boxes, a red one, a white one and a blue one, so that each box contains at least one card.*

A member of the audience selects two of the three boxes, chooses one card from each and announces the sum of the numbers on the chosen cards. Given this sum, the magician identifies the box from which no card has been chosen.

How many ways are there to put all the cards into boxes so that this trick always works? (Two ways are considered different if at least one card is put into a different box.)

Solution: There are 12 ways. If the boxes are denoted R, W, B, then the 2 basic configurations are

$$R = \{1, 4, 7, \ldots, 100\}, \quad W = \{2, 5, 8, \ldots, 98\}, \quad B = \{3, 6, 9, \ldots, 99\},$$

and

$$R = \{1\}, \quad W = \{2, 3, 4, \ldots, 99\}, \quad B = \{100\},$$

and the 12 solutions consists of the 6 permutations of each basic configuration.

Proof: Let the boxes be A, B, C. One first notes that $n \mapsto 101 - n$ preserves $\{1, 2, \ldots, 100\}$, and in the following, the expression "by symmetry" will include this map. One begins the proof with the following useful result.

Lemma 4.1. *If A, B, C satisfy the conditions of the problem, and a and $a+k$ are in A, then it is not possible to have b in B such that $b+k$ is in C.*

Proof: In fact, it is easily seen that this is equivalent to the conditions of the problem. Thus, if $b \in B$ and $c+k \in C$, then $a+b+k$ is in $A+B$ and in $A+C$, which is not allowed. □

Lemma 4.2. *If A, B, C satisfy the conditions of the problem, and A contains a and $a+k$ and box B contains b and $b+k$, then if c is in C and $1 \le c+k \le 100$, then $c+k$ is in C.*

Proof: One applies Lemma 4.1 twice. Thus, applying it with respect to A shows that $c+k$ cannot be in B, and applying it with respect to B shows that $c+k$ cannot be in A. The result follows. □

Lemma 4.3. *Let A, B, C satisfy the conditions of the problem , then it is not possible to have $a, a+k \in A$ and $b, b+k \in B$, where $k = 1$ or $k = 2$.*

Proof: Assume that such a and b existed. Then C would have an element c such that $1 \le c+k \le 100$ or $1 \le c-k \le 100$, so there would exist a c' such that $c'+k \in C$. It would follow from Lemma 4.2 that $1 \le a \pm rk \le 100$, $r \in \mathbf{Z}$, are all in A and similarly, $1 \le b \pm rk \le 100$, $r \in \mathbf{Z}$, are all in B, $1 \le c \pm rk \le 100$, $r \in \mathbf{Z}$, are all in C. If $k = 1$, then each set has 100 elements while if $k = 2$, each set has 50 elements, so A, B, C do not form a partition of $\{1, 2, 3, \ldots, 100\}$. This contradiction proves the result. □

The proof will now be split up according to the minimum of all the differences of two elements which are in a same box.

(a) The minimum is 1. Without loss of generality, say that $a, a+1 \in A$. Now either B and C are of the form $\{1\}$ and $\{100\}$, or there exists (without loss of generality) $b \in B$ such that $1 < b < 100$ and (by the symmetry $n \mapsto 101-n$) a $c \in C$ such that $c < 100$.

By Lemma 4.3, $b+1$ and $c+1$ are in A. It follows that $b+c+1$ is in $A+B$ and in $A+C$, which is not allowed. This possibility is therefore excluded unless B and C are of the form $\{1\}$ and $\{100\}$.

(b) The minimum is 2. Without loss of generality, let $a, a+2 \in A$. Since the minimum is 2, $a+1$ is not in A and, without loss of generality, let $a+1 \in B$. Now either $a+3 \le 100$ or $a-1 \ge 1$. By symmetry $(n \mapsto 101-n)$, assume that $a+3 \le 100$. By Lemma 4.1, one cannot have $a+3 \in C$. By Lemma 4.2, one cannot have $a+3$ in B, and by part (a), one cannot have $a+3 \in A$, since $a+2 \in A$. This case is therefore excluded.

(c) The minimum is 3. Since A, B, C form a partition of $\{1, 2, \ldots, 100\}$, one of these sets must have at least 34 members, since otherwise, one would have $|A|+|B|+|C| \le 33+33+33 = 99$. Without loss of generality, let this set be A. Now split up A into 33 bins $\{1, 2, 3\}$, $\{4, 5, 6\}$,…,$\{97, 98, 99\}$. Since the minimum difference of elements of A is 3, each bin can have at most one element. But since there are more than 33 elements, and only 100 is left over, each bin has one element, thus exactly one element. Since there are at least 34 elements, it follows that 100 is in A. Since $100 \in A$, one cannot have 98 or 99 in A, and therefore $97 \in A$. Similarly, one has $94, \ldots, 7, 4, 1 \in A$. It follows that $A = \{1, 4, 7, \ldots, 100\}$.

A similar argument shows that B and C are $\{2, 5, \ldots, 98\}$ and $\{3, 6, \ldots, 99\}$ in some order.

(d) The minimum is > 3. This is not possible, as one of the boxes has at least 34 elements, and thus minimum difference ≤ 3, by the argument used in (c).

Remark 4.1. Harry Tamvakis has found the following simpler argument. His argument begins by considering the general problem with cards numbered 1 to n. One also shows that there are only two types of solutions, i.e., one with $\{3a+k\}$, $k = 0, 1, 2$, and $\{1\}$, $\{2, \ldots, n-1\}$, $\{n\}$, but the main point is that the first type of solution is *stable* under $n \mapsto n+1$,(by adding the card numbered $n+1$ to the solution with n cards), while the second is not. This observation yields a simple induction argument: Assume that the result holds for n, then given a legal configuration with $n+1$ cards, remove card $n+1$ from the boxes. This is a solution for n cards and therefore of first type, unless removing card $n+1$ left one box empty. In the first case, one easily shows that card $n+1$ must fit into the correct arithmetic progression modulo 3, yielding the first type of solution. In the second case, one similarly removes card 1 from the boxes which shows that its box only contained this one card, and one gets the second solution.

Problem 5. *Determine whether or not there exists a positive integer n divisible by exactly 2000 different prime numbers, and $2^n + 1$ is divisible by n.*

Solution: Yes, there exists such a number. In fact, for any positive integer k, there exists a positive integer n_k divisible by exactly k different prime numbers such that n_k divides $2^{n_k}+1$.

Proof: The proof is by induction. The induction starts with $k=1$, and with $n_1=3$, since 3 divides $9=2^3+1$.

Now assume that n_k has been constructed with n_k dividing $2^{n_k}+1$, and n_k having exactly k different prime factors. To construct of n_{k+1}, one uses the following steps (for ease of notation, let $N=n_k$):

(a) If p^β is the largest power of p dividing N and p^β is the largest power of p dividing 2^N+1, then $p^{\alpha+\beta}$ is the largest power of p dividing $2^{N^2}+1$.

(b) N^2 divides $2^{N^2}+1$.

(c) There is a prime q not dividing N but dividing $2^{N^2}+1$.

(d) Let $n_{k+1}=N^2q$, then n_{k+1} satisfies the above conditions.

Proof of (a): Let p be any prime dividing N with p^α and p^β as defined in (a). One can therefore write $2^N=A\,p^\beta-1$, for some integer A not divisible by p. One now uses the binomial theorem to compute

$$(2^N)^p=(A\,p^\beta-1)^p=A'\,p^{\beta+2}+A\,p^{\beta+1}-1=A_1\,p^{\beta+1}-1\,,$$

for some integer $A_1=A'\,p+A$ not divisible by p. Iterating this gives $(2^N)^{p^\alpha}=A_\alpha\,p^{\alpha+\beta}-1$, for some integer A_α not divisible by p. Similarly,

$$2^{N^2}=((2^N)^{p^\alpha})^{N/p^\alpha}=(A_\alpha\,p^{\alpha+\beta}-1)^{N/p^\alpha}=A''\,p^{\alpha+\beta+1}+A_\alpha\left(\frac{N}{p^\alpha}\right)p^{\alpha+\beta}-1.$$

Since A_α is not divisible by p and, by definition, N/p^α is not divisible by p, it follows that $2^{N^2}+1$ is divisible by $p^{\alpha+\beta}$, but by no higher power, as claimed.

Proof of (b): Note that, by assumption, $\beta\ge\alpha$, so one has that $p^{2\alpha}$ divides $2^{N^2}+1$. Since this holds for every p dividing N, it follows that N^2 divides $2^{N^2}+1$.

Proof of (c): Let M be the largest divisor of 2^N+1 such that M is divisible only by primes which divide N. Similarly, let M' be the largest divisor of $2^{N^2}+1$, such that M' is divisible only by primes which divide N. It follows from part (a) that $M'=MN$, since part (a) proves this for each separate prime power dividing N. Since M and N both divide 2^N+1 it follows that both M and N are smaller or equal to 2^N+1. Therefore

$$M'=MN\le(2^N+1)^2\le(2^{N+1})^2=2^{2N+2}\,.$$

On the other hand, using $N\ge3$,

$$2^{N^2}=(2^{2N})^{N/2}=2^{2N}\,(2^{2N(N/2-1)}\ge2^{2N+3}\,,$$

since $N/2-1\ge3/2$ and thus $2N(N/2-1)\ge3$. It follows that $M'<2^{N^2}+1$, and thus $2^{N^2}+1$ must be divisible by a prime q which does not divide N.

Proof of (d): Let $n_{k+1}=N^2\,q$. Then by (b) one has $2^{N^2}\equiv-1\ (\mathrm{mod}\,N^2)$ so that

$$2^{n_{k+1}}\equiv(-1)^q=-1\ (\mathrm{mod}\,N^2)\,,$$

recalling that q must be odd since it divides a power of 2 plus 1. By the choice of q, one also has that $2^{N^2} \equiv -1 \pmod q$ so that

$$2^{n_{k+1}} \equiv (-1)^q = -1 \pmod q\,.$$

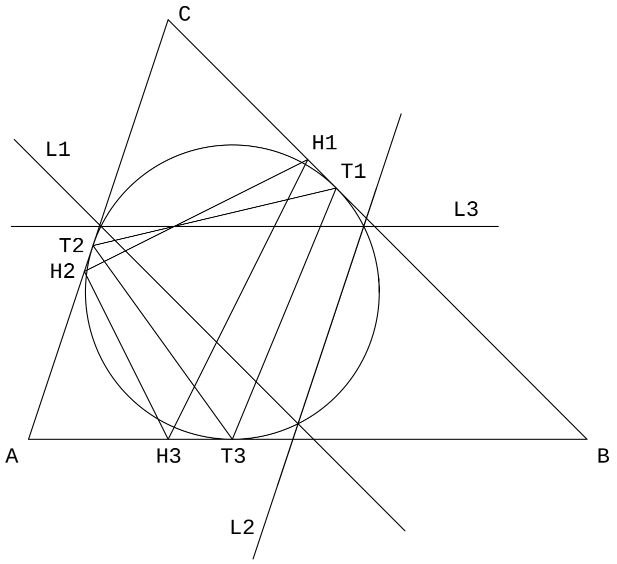
The result follows from the Chinese Remainder Theorem.

Remark 5.1. The statement of the problem can be interpreted to mean: "n is divisible by exactly 2000 different prime numbers, each with multiplicity one," In other words, n is assumed to be squarefree. It is conceivable that a more precise form of the question was avoided in order not to give away the idea of the solution, which depends on having primes with high multiplicities.

The alternate question appears to be intractable, in the nature of resolving whether there are an infinite number of primes of the form $2^p - 1$. See [4] for examples of these types of unsolved problems.

Problem 6. *Let AH_1, BH_2, CH_3 be the altitudes of an acute–angled triangle ABC. The incircle of the triangle ABC touches the sides BC, CA, AB at T_1, T_2, T_3, respectively. Let the lines ℓ_1, ℓ_2, ℓ_3 be the reflections of the lines H_2H_3, H_3H_1, H_1H_2 in the lines T_2T_3, T_3T_1, T_1T_2, respectively.*

Prove that ℓ_1, ℓ_2, ℓ_3 determine a triangle whose vertices lie on the incircle of the triangle ABC.



Solution: The solution requires some basic results from triangle geometry which are easy to prove, but which will only be quoted here.

Theorem 6.1. *Let the notation be as in the statement of Problem 6. Then*

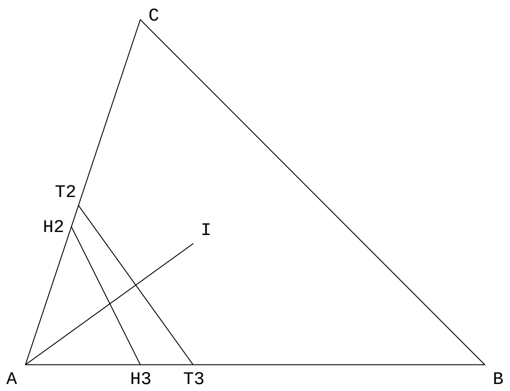
(a) The center of the incircle is the intersection of the bisectors of angles A, B, C.

(b) The center of the circumcircle is the intersection of the right bisectors of the sides AB, BC, CA.

(c) The triangle AH_2H_3 is similar to the triangle ABC, i.e., corresponding angles are equal. Similar statements hold for BH_3H_1, and CH_1H_2.

These results immediately allow some progress.

Lemma 6.1. *Let the notation be as in the statement of Problem 6, then ℓ_1, ℓ_2, ℓ_3 determine a triangle (possibly a point) similar to triangle ABC.*



Proof: Let I be the center of the incircle. Since AH_2H_3 is similar to ABC, and AI bisects the angle BAC, reflecting H_2H_3 about AI makes it parallel to BC. Since T_2T_3 is perpendicular to AI, it follows that reflecting H_2H_3 about T_2T_3 also makes it parallel to BC, since two reflections along two perpendicular axes is equivalent to one rotation of 180 degrees. Thus, ℓ_1 is parallel to BC. Similarly, ℓ_2 is parallel to AC and ℓ_3 is parallel to AB. Note also that ℓ_1 opposite angle A, ℓ_2 opposite B, and ℓ_3 opposite B. □

In order to proceed, one introduces coordinates for points inside a triangle by their distance from the sides. Thus, a point P inside the triangle ABC will be denoted by (x, y, z), where x, y, z are the distances from P to BC, AC, and AB, respectively (since the triangle is assumed to be acute, the question of signs does not arise). Note that P is uniquely determined by any two of x, y, z.

Remark 6.1. This parametrization corresponds to the usual barycentric coordinates since it is easy to show that, with h_1 the length of AH_1, etc., one has

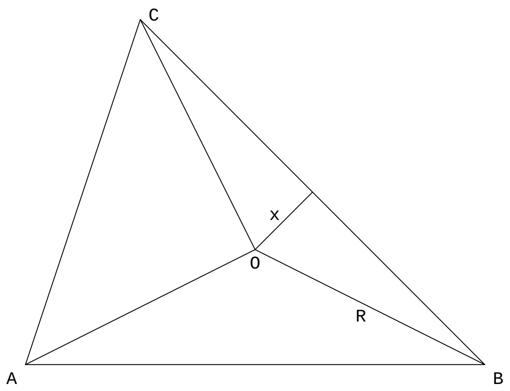
$$P = \frac{x}{h_1} A + \frac{y}{h_2} B + \frac{z}{h_3} C\,, \quad \text{where} \quad \frac{x}{h_1} + \frac{y}{h_2} + \frac{z}{h_3} = 1\,.$$

The advantage of this parametrization is that it characterizes the incenter and circumcenter from knowledge of the sides alone.

Lemma 6.2. *Let the notation be as in the statement of Problem 6, and P a point in the triangle with coordinates (x, y, z).*

(a) If $(x, y, z) = (r, r, r)$, then P is center of the incircle of the triangle and r the radius of the incircle.

(b) If $(x, y, z) = (R\, \cos A, R\, \cos B, R\, \sin C)$, where $A = \angle BAC$ etc., then P is the center of the circumcircle of the triangle and R the radius of the circumcircle.



Proof: Part (a) is trivial. To prove part (b), let O be the center of the circumcircle. Since triangle ABC is acute, O lies inside the triangle, and $R = |OB|$ is the radius of the circumcircle. Let α be $\angle OBC = \angle OBC$, so that $x = R\,\sin\alpha$. Furthermore, let $\beta = \angle OCA = \angle OAC$ and $\gamma = \angle OAB = \angle OBA$. Since $2\,(\alpha+\beta+\gamma) = 180^{\text{o}}$ it follows that $\alpha = 90^{\text{o}} - (\beta+\gamma)$. But also, one has $\beta+\gamma = \angle A$ so that $\sin\alpha = \cos A$. The result follows. $\square$

The final result follows directly from

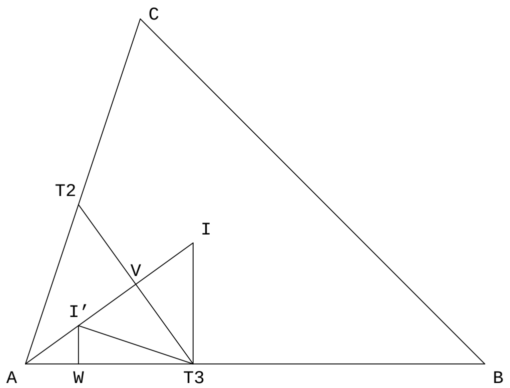
Lemma 6.3. *Let the notation be as in the statement of Problem 6, and let I' be the reflection of I, the center of the incircle, through the line T_2T_3. Then I' is the center of the incircle of AH_2H_3.*

Indeed, assume that Lemma 6.3 holds. Then the distance between I' and the line H_2H_3 is the radius of the incircle of triangle AH_2H_3. By Theorem 6.1 (c), this triangle is similar to triangle ABC, so its inradius is the inradius of ABC multiplied by the factor of similarity. By Theorem 6.1 (c), the factor of similarity is $|AH_3|/|AC| = \cos A$, since CH_3 is an altitude. It follows that the distance from I' to the line H_2H_3 is $r\,\cos A$.

One now notes that, the distance from I', the reflection of I through T_2T_3, to the line H_2H_3 is exactly the same as the distance between I and the line ℓ_1, the reflection of H_2H_3 through T_2T_3. One concludes that the distance from I to ℓ_1 is $r\,\cos A$. Similarly, the distance from I to ℓ_2 is $r\,\cos B$ and the distance from I to ℓ_3 is $r\,\cos C$.

Lemma 6.1 and Lemma 6.2 (b) show that I is the center of the circumcircle of the triangle with sides ℓ_1, ℓ_2, ℓ_3, and that this circle has radius r. The result is therefore proved, given that Lemma 6.3 holds.

Proof of Lemma 6.3: In order to prove this, one uses the fact just proved above that the triangle AH_2H_3 has ratio of similarity $\cos A$ with respect to triangle ABC, so has inradius $r\,\cos A$, and then apply Lemma 6.2 (A).



One therefore needs to compute the distance from I' to AB. Thus, let W be the point on AB such that AWI' is a right angle. The axis of reflection T_2T_3 cuts the line AI perpendicularly, so that $r = |T_3I| = |T_3I'|$. It follows that $|I'W| = r\,\cos\angle T_3I'W$.

Let $\delta = \angle BAI$. Since AWI' is a right angle, $\angle AI'W$ and $\angle AIT_3$ are both equal to $90^{\text{o}} - \delta$. Since $|T_3I| = |T_3I'|$, one also has $\angle T_3I'I = 90^{\text{o}} - \delta$. It follows that $\angle T_3I'W = 2\delta$ and thus $|I'W| = r\,\cos(2\delta)$.

By Theorem 6.1 (a), the line AI bisects $\angle A$, so it follows that $|I'W| = r\,\cos A$. Moreover, the fact that this line bisects $\angle BAC$ implies that the distance from I' to AC is also $r\,\cos A$. Since two distances to the sides determine a point uniquely and the inradius is $r\,\cos A$, it follows that I' is the center of the incircle, as claimed. $\square$

Remark 6.2. The above proof relies on two results: Lemma 6.1 and Lemma 6.3. The first is "soft" in the sense that it follows from known results without any computation. The second is the heart of the technical argument and appears to be of independent interest.

Remark 6.3. The above argument was discovered only after a using a brute force algebraic method to prove the result. The following is a brief outline of this method.

Without loss of generality, one can assume that $A = (0,0)$, $B = (1,0)$, and $C = (m,n)$, where $0 < m < 1$ and $n > 0$. Furthermore, let $a = \sqrt{(1-m)^2 + n^2}$ be the length of the side opposite A, and $b = \sqrt{m^2 + n^2}$ the length of the side opposite B, and $p = 1 + b + c$ the perimeter of the triangle.

Once again, let the center of the incircle be I, then it is easily computed that I has coordinates $((m + b)/p, n/p)$, and so $r = n/p$. If V is once again the intersection of T_2T_3 with AI, then $V = \frac{m+b}{2b} I$.

The reflection of a point U about T_2T_3 is given by $U \mapsto U + 2\left(1 - \frac{U \cdot V}{\|V\|^2}\right) V$. Thus, if H_2' and H_3' are the images of H_2 and H_3 under a reflection through T_2T_3, then $H_2' = \frac{-m}{b} B + 2V$ and $H_3' = \frac{-m}{b} C + 2V$.

A computation shows that line ℓ_1 has equation

$$y = \frac{n}{m-1} x + \frac{n}{bp(m-1)} \left(ma - b(b+1)\right).$$

One can now derive the equation of ℓ_2 by using the symmetry $x \mapsto 1 - x$ which takes $a \mapsto b$ and $m \mapsto 1 - m$. It follows that ℓ_2 has equation

$$y = \frac{n}{m} x - \frac{n}{m} - \frac{n}{apm}((1-m)b - a(a+1)).$$

Fairly straightforward algebraic computation eventually yields the coordinates (x', y') of the intersection of ℓ_1 and ℓ_2, which are

$$x' = \frac{b^2(m-1)^2 - a^2m^2}{abp} + \frac{b+m}{p}, \quad y' = \frac{n\left(b^2(m-1) - a^2m\right)}{abp} + \frac{n}{p}.$$

Since $I = ((b+m)/p, n/p)$, it is then easy to check that (x', y') is at distance $r = n/p$ from I. Since this holds for any two vertices, the result is proved.

References

[1] J.–P. Boudine, F. Lo Jacomo, R. Cuculière, *Olympiades Internationales de Mathématiques, Énoncés et solutions détaillés, Années 1988 à 1997,* Édition du Choix, Marseille, 1998.

[2] H.S.M. Coxeter and S.L. Greitzer, *Geometry Revisited,* Mathematical Association of America, 1967.

[3] S.L. Greitzer, editor, *International Mathematical Olympiads, 1959–1977,* Mathematical Association of America, 1979.

[4] R.K. Guy, "Unsolved problems in number theory, 2nd Edition." Unsolved Problems in Intuitive Mathematics, I. Springer–Verlag, New York, 1994.

[5] M.S. Klamkin, editor, *International Mathematical Olympiads. 1978–1985, and Forty Supplementary problems,* Mathematical Association of America, 1999.

[6] International Mathematics Olympiad, web site: `olympiads.win.tue.nl/imo/`

[7] J. Scholes, 41st IMO 2000, `www.kalva.demon.co.uk/imo/imo00.html`.

[8] A. Shen, *Entrance Examinations to the Mekh–mat,* Mathematical Intelligencer **16** (1994), 6–10.

[9] I. Vardi, *Mekh–mat entrance examination problems,* IHES preprint IHES/M/00/06, January 2000.

[10] D. Zeilberger, *Identities in search of identity,* J. Theoretical Computer Science **117** (1993), 23–38.