

35<sup>th</sup> United States of America Mathematical Olympiad

1. Let  $p$  be a prime number and let  $s$  be an integer with  $0 < s < p$ . Prove that there exist integers  $m$  and  $n$  with  $0 < m < n < p$  and

$$\left\{ \frac{sm}{p} \right\} < \left\{ \frac{sn}{p} \right\} < \frac{s}{p}$$

if and only if  $s$  is not a divisor of  $p - 1$ .

(For  $x$  a real number, let  $\lfloor x \rfloor$  denote the greatest integer less than or equal to  $x$ , and let  $\{x\} = x - \lfloor x \rfloor$  denote the fractional part of  $x$ .)

**First Solution.** First suppose that  $s$  is a divisor of  $p - 1$ ; write  $d = (p - 1)/s$ . As  $x$  varies among  $1, 2, \dots, p - 1$ ,  $\{sx/p\}$  takes the values  $1/p, 2/p, \dots, (p - 1)/p$  once each in some order. The possible values with  $\{sx/p\} < s/p$  are precisely  $1/p, \dots, (s - 1)/p$ . From the fact that  $\{sd/p\} = (p - 1)/p$ , we realize that the values  $\{sx/p\} = (p - 1)/p, (p - 2)/p, \dots, (p - s + 1)/p$  occur for

$$x = d, 2d, \dots, (s - 1)d$$

(which are all between 0 and  $p$ ), and so the values  $\{sx/p\} = 1/p, 2/p, \dots, (s - 1)/p$  occur for

$$x = p - d, p - 2d, \dots, p - (s - 1)d,$$

respectively. From this it is clear that  $m$  and  $n$  cannot exist as requested.

Conversely, suppose that  $s$  is not a divisor of  $p - 1$ . Put  $m = \lceil p/s \rceil$ ; then  $m$  is the smallest positive integer such that  $\{ms/p\} < s/p$ , and in fact  $\{ms/p\} = (ms - p)/p$ . However, we cannot have  $\{ms/p\} = (s - 1)/p$  or else we would have  $(m - 1)s = p - 1$ , contradicting our hypothesis that  $s$  does not divide  $p - 1$ . Hence the unique  $n \in \{1, \dots, p - 1\}$  for which  $\{nx/p\} = (s - 1)/p$  has the desired properties (since the fact that  $\{nx/p\} < s/p$  forces  $n \geq m$ , but  $m \neq n$ ).

**Second Solution.** We prove the contrapositive statement:

Let  $p$  be a prime number and let  $s$  be an integer with  $0 < s < p$ . Prove that the following statements are equivalent:

- (a)  $s$  is a divisor of  $p - 1$ ;

(b) if integers  $m$  and  $n$  are such that  $0 < m < p$ ,  $0 < n < p$ , and

$$\left\{ \frac{sm}{p} \right\} < \left\{ \frac{sn}{p} \right\} < \frac{s}{p},$$

then  $0 < n < m < p$ .

Since  $p$  is prime and  $0 < s < p$ ,  $s$  is relatively prime to  $p$  and

$$S = \{s, 2s, \dots, (p-1)s, ps\}$$

is a set of complete residues classes modulo  $p$ . In particular,

- (1) there is a unique integer  $d$  with  $0 < d < p$  such that  $sd \equiv -1 \pmod{p}$ ; and
- (2) for every  $k$  with  $0 < k < p$ , there exists a unique pair of integers  $(m_k, a_k)$  with  $0 < m_k < p$  such that  $m_k s + a_k p = k$ .

Now we consider the equations

$$m_1 s + a_1 p = 1, \quad m_2 s + a_2 p = 2, \quad \dots, \quad m_s s + a_s p = s.$$

Hence  $\{m_k s/p\} = k/p$  for  $1 \leq k \leq s$ .

Statement (b) holds if and only if  $0 < m_s < m_{s-1} < \dots < m_1 < p$ . For  $1 \leq k \leq s-1$ ,  $m_k s - m_{k+1} s = (a_{k+1} - a_k)p - 1$ , or  $(m_k - m_{k+1})s \equiv -1 \pmod{p}$ . Since  $0 < m_{k+1} < m_k < p$ , by (1), we have  $m_k - m_{k+1} = d$ . We conclude that (b) holds if and only if  $m_s, m_{s-1}, \dots, m_1$  form an arithmetic progression with common difference  $-d$ . Clearly  $m_s = 1$ , so  $m_1 = 1 + (s-1)d = jp - d + 1$  for some  $j$ . Then  $j = 1$  because  $m_1$  and  $d$  are both positive and less than  $p$ , so  $sd = p - 1$ . This proves (a).

Conversely, if (a) holds, then  $sd = p - 1$  and  $m_k \equiv -d s m_k \equiv -dk \pmod{p}$ . Hence  $m_k = p - dk$  for  $1 \leq k \leq s$ . Thus  $m_s, m_{s-1}, \dots, m_1$  form an arithmetic progression with common difference  $-d$ . Hence (b) holds.

This problem was proposed by Kiran Kedlaya.

2. For a given positive integer  $k$  find, in terms of  $k$ , the minimum value of  $N$  for which there is a set of  $2k + 1$  distinct positive integers that has sum greater than  $N$  but every subset of size  $k$  has sum at most  $N/2$ .

**Solution.** The minimum is  $N = 2k^3 + 3k^2 + 3k$ . The set

$$\{k^2 + 1, k^2 + 2, \dots, k^2 + 2k + 1\}$$

has sum  $2k^3 + 3k^2 + 3k + 1 = N + 1$  which exceeds  $N$ , but the sum of the  $k$  largest elements is only  $(2k^3 + 3k^2 + 3k)/2 = N/2$ . Thus this  $N$  is such a value.

Suppose  $N < 2k^3 + 3k^2 + 3k$  and there are positive integers  $a_1 < a_2 < \cdots < a_{2k+1}$  with  $a_1 + a_2 + \cdots + a_{2k+1} > N$  and  $a_{k+2} + \cdots + a_{2k+1} \leq N/2$ . Then

$$(a_{k+1} + 1) + (a_{k+1} + 2) + \cdots + (a_{k+1} + k) \leq a_{k+2} + \cdots + a_{2k+1} \leq N/2 < \frac{2k^3 + 3k^2 + 3k}{2}.$$

This rearranges to give  $2ka_{k+1} \leq N - k^2 - k$  and  $a_{k+1} < k^2 + k + 1$ . Hence  $a_{k+1} \leq k^2 + k$ . Combining these we get

$$2(k+1)a_{k+1} \leq N + k^2 + k.$$

We also have

$$(a_{k+1} - k) + \cdots + (a_{k+1} - 1) + a_{k+1} \geq a_1 + \cdots + a_{k+1} > N/2$$

or  $2(k+1)a_{k+1} > N + k^2 + k$ . This contradicts the previous inequality, hence no such set exists for  $N < 2k^3 + 3k^2 + 3k$  and the stated value is the minimum.

This problem was proposed by Dick Gibbs.

3. For integral  $m$ , let  $p(m)$  be the greatest prime divisor of  $m$ . By convention, we set  $p(\pm 1) = 1$  and  $p(0) = \infty$ . Find all polynomials  $f$  with integer coefficients such that the sequence  $\{p(f(n^2)) - 2n\}_{n \geq 0}$  is bounded above. (In particular, this requires  $f(n^2) \neq 0$  for  $n \geq 0$ .)

**Solution.** The polynomial  $f$  has the required properties if and only if

$$f(x) = c(4x - a_1^2)(4x - a_2^2) \cdots (4x - a_k^2), \tag{*}$$

where  $a_1, a_2, \dots, a_k$  are odd positive integers and  $c$  is a nonzero integer. It is straightforward to verify that polynomials given by (\*) have the required property. If  $p$  is a prime divisor of  $f(n^2)$  but not of  $c$ , then  $p|(2n - a_j)$  or  $p|(2n + a_j)$  for some  $j \leq k$ . Hence  $p - 2n \leq \max\{a_1, a_2, \dots, a_k\}$ . The prime divisors of  $c$  form a finite set and do affect whether or not the given sequence is bounded above. The rest of the proof is devoted to showing that any  $f$  for which  $\{p(f(n^2)) - 2n\}_{n \geq 0}$  is bounded above is given by (\*).

Let  $\mathbb{Z}[x]$  denote the set of all polynomials with integral coefficients. Given  $f \in \mathbb{Z}[x]$ , let  $\mathcal{P}(f)$  denote the set of those primes that divide at least one of the numbers in the sequence  $\{f(n)\}_{n \geq 0}$ . The solution is based on the following lemma.

**Lemma.** *If  $f \in \mathbb{Z}[x]$  is a nonconstant polynomial then  $\mathcal{P}(f)$  is infinite.*

*Proof.* Repeated use will be made of the following basic fact: if  $a$  and  $b$  are distinct integers and  $f \in \mathbb{Z}[x]$ , then  $a - b$  divides  $f(a) - f(b)$ . If  $f(0) = 0$ , then  $p$  divides  $f(p)$  for every prime  $p$ , so  $\mathcal{P}(f)$  is infinite. If  $f(0) = 1$ , then every prime divisor  $p$  of  $f(n!)$  satisfies  $p > n$ . Otherwise  $p$  divides  $n!$ , which in turn divides  $f(n!) - f(0) = f(n!) - 1$ . This yields  $p|1$ , which is false. Hence  $f(0) = 1$  implies that  $\mathcal{P}(f)$  is infinite. To complete the proof, set  $g(x) = f(f(0)x)/f(0)$  and observe that  $g \in \mathbb{Z}[x]$  and  $g(0) = 1$ . The preceding argument shows that  $\mathcal{P}(g)$  is infinite, and it follows that  $\mathcal{P}(f)$  is infinite.  $\square$

Suppose  $f \in \mathbb{Z}[x]$  is nonconstant and there exists a number  $M$  such that  $p(f(n^2)) - 2n \leq M$  for all  $n \geq 0$ . Application of the lemma to  $f(x^2)$  shows that there is an infinite sequence of distinct primes  $\{p_j\}$  and a corresponding infinite sequence of nonnegative integers  $\{k_j\}$  such that  $p_j | f(k_j^2)$  for all  $j \geq 1$ . Consider the sequence  $\{r_j\}$  where  $r_j = \min\{k_j \pmod{p_j}, p_j - k_j \pmod{p_j}\}$ . Then  $0 \leq r_j \leq (p_j - 1)/2$  and  $p_j | f(r_j^2)$ . Hence  $2r_j + 1 \leq p_j \leq p(f(r_j^2)) \leq M + 2r_j$ , so  $1 \leq p_j - 2r_j \leq M$  for all  $j \geq 1$ . It follows that there is an integer  $a_1$  such that  $1 \leq a_1 \leq M$  and  $a_1 = p_j - 2r_j$  for infinitely many  $j$ . Let  $m = \deg f$ . Then  $p_j | 4^m f((p_j - a_1)/2)^2$  and  $4^m f((x - a_1)/2)^2 \in \mathbb{Z}[x]$ . Consequently,  $p_j | f((a_1/2)^2)$  for infinitely many  $j$ , which shows that  $(a_1/2)^2$  is a zero of  $f$ . Since  $f(n^2) \neq 0$  for  $n \geq 0$ ,  $a_1$  must be odd. Then  $f(x) = (4x - a_1^2)g(x)$  where  $g \in \mathbb{Z}[x]$ . (See the note below.) Observe that  $\{p(g(n^2)) - 2n\}_{n \geq 0}$  must be bounded above. If  $g$  is constant, we are done. If  $g$  is nonconstant, the argument can be repeated to show that  $f$  is given by (\*).

*Note.* The step that gives  $f(x) = (4x - a_1^2)g(x)$  where  $g \in \mathbb{Z}[x]$  follows immediately using a lemma of Gauss. The use of such an advanced result can be avoided by first writing  $f(x) = r(4x - a_1^2)g(x)$  where  $r$  is rational and  $g \in \mathbb{Z}[x]$ . Then continuation gives  $f(x) = c(4x - a_1^2) \cdots (4x - a_k^2)$  where  $c$  is rational and the  $a_i$  are odd. Consideration of the leading coefficient shows that the denominator of  $c$  is  $2^s$  for some  $s \geq 0$  and consideration of the constant term shows that the denominator is odd. Hence  $c$  is an integer.

This problem was proposed by Titu Andreescu and Gabriel Dospinescu.

4. Find all positive integers  $n$  such that there are  $k \geq 2$  positive rational numbers  $a_1, a_2, \dots, a_k$  satisfying  $a_1 + a_2 + \cdots + a_k = a_1 \cdot a_2 \cdots a_k = n$ .

**Solution.** The answer is  $n = 4$  or  $n \geq 6$ .

**I.** First, we prove that each  $n \in \{4, 6, 7, 8, 9, \dots\}$  satisfies the condition.

(1). If  $n = 2k \geq 4$  is even, we set  $(a_1, a_2, \dots, a_k) = (k, 2, 1, \dots, 1)$ :

$$a_1 + a_2 + \dots + a_k = k + 2 + 1 \cdot (k - 2) = 2k = n,$$

and

$$a_1 \cdot a_2 \cdot \dots \cdot a_k = 2k = n .$$

(2). If  $n = 2k + 3 \geq 9$  is odd, we set  $(a_1, a_2, \dots, a_k) = \left(k + \frac{3}{2}, \frac{1}{2}, 4, 1, \dots, 1\right)$ :

$$a_1 + a_2 + \dots + a_k = k + \frac{3}{2} + \frac{1}{2} + 4 + (k - 3) = 2k + 3 = n,$$

and

$$a_1 \cdot a_2 \cdot \dots \cdot a_k = \left(k + \frac{3}{2}\right) \cdot \frac{1}{2} \cdot 4 = 2k + 3 = n .$$

(3). A very special case is  $n = 7$ , in which we set  $(a_1, a_2, a_3) = \left(\frac{4}{3}, \frac{7}{6}, \frac{9}{2}\right)$ . It is also easy to check that

$$a_1 + a_2 + a_3 = a_1 \cdot a_2 \cdot a_3 = 7 = n.$$

**II.** Second, we prove by contradiction that each  $n \in \{1, 2, 3, 5\}$  fails to satisfy the condition.

Suppose, on the contrary, that there is a set of  $k \geq 2$  positive rational numbers whose sum and product are both  $n \in \{1, 2, 3, 5\}$ . By the Arithmetic-Geometric Mean inequality, we have

$$n^{1/k} = \sqrt[k]{a_1 \cdot a_2 \cdot \dots \cdot a_k} \leq \frac{a_1 + a_2 + \dots + a_k}{k} = \frac{n}{k},$$

which gives

$$n \geq k^{\frac{k}{k-1}} = k^{1+\frac{1}{k-1}} .$$

Note that  $n > 5$  whenever  $k = 3, 4$ , or  $k \geq 5$ :

$$k = 3 \Rightarrow n \geq 3\sqrt{3} = 5.196... > 5;$$

$$k = 4 \Rightarrow n \geq 4\sqrt[3]{4} = 6.349... > 5;$$

$$k \geq 5 \Rightarrow n \geq 5^{1+\frac{1}{k-1}} > 5 .$$

This proves that none of the integers 1, 2, 3, or 5 can be represented as the sum and, at the same time, as the product of three or more positive numbers  $a_1, a_2, \dots, a_k$ , rational or irrational.

The remaining case  $k = 2$  also goes to a contradiction. Indeed,  $a_1 + a_2 = a_1 a_2 = n$  implies that  $n = a_1^2 / (a_1 - 1)$  and thus  $a_1$  satisfies the quadratic

$$a_1^2 - na_1 + n = 0 .$$

Since  $a_1$  is supposed to be *rational*, the discriminant  $n^2 - 4n$  must be a perfect square (a square of a positive integer). However, it can be easily checked that this is not the case for any  $n \in \{1, 2, 3, 5\}$ . This completes the proof.

**Remark.** Actually, among all positive integers only  $n = 4$  can be represented both as the sum and product of the same two rational numbers. Indeed,  $(n - 3)^2 < n^2 - 4n = (n - 2)^2 - 4 < (n - 2)^2$  whenever  $n \geq 5$ ; and  $n^2 - 4n < 0$  for  $n = 1, 2, 3$ .

This problem was proposed by Ricky Liu.

5. A mathematical frog jumps along the number line. The frog starts at 1, and jumps according to the following rule: if the frog is at integer  $n$ , then it can jump either to  $n + 1$  or to  $n + 2^{m_n+1}$  where  $2^{m_n}$  is the largest power of 2 that is a factor of  $n$ . Show that if  $k \geq 2$  is a positive integer and  $i$  is a nonnegative integer, then the minimum number of jumps needed to reach  $2^i k$  is greater than the minimum number of jumps needed to reach  $2^i$ .

**First Solution.** For  $i \geq 0$  and  $k \geq 1$ , let  $x_{i,k}$  denote the minimum number of jumps needed to reach the integer  $n_{i,k} = 2^i k$ . We must prove that

$$x_{i,k} > x_{i,1} \tag{1}$$

for all  $i \geq 0$  and  $k \geq 2$ . We prove this using the method of descent.

First note that (1) holds for  $i = 0$  and all  $k \geq 2$ , because it takes 0 jumps to reach the starting value  $n_{0,1} = 1$ , and at least one jump to reach  $n_{0,k} = k \geq 2$ . Now assume that that (1) is not true for all choices of  $i$  and  $k$ . Let  $i_0$  be the minimal value of  $i$  for which (1) fails for some  $k$ , let  $k_0$  be the minimal value of  $k > 1$  for which  $x_{i_0,k} \leq x_{i_0,1}$ . Then it must be the case that  $i_0 \geq 1$  and  $k_0 \geq 2$ .

Let  $J_{i_0,k_0}$  be a shortest sequence of  $x_{i_0,k_0} + 1$  integers that the frog occupies in jumping from 1 to  $2^{i_0} k_0$ . The length of each jump, that is, the difference between consecutive integers in  $J_{i_0,k_0}$ , is either 1 or a positive integer power of 2. The sequence  $J_{i_0,k_0}$  cannot contain  $2^{i_0}$  because it takes more jumps to reach  $2^{i_0} k_0$  than it does to reach  $2^{i_0}$ . Let  $2^{M+1}$ ,  $M \geq 0$

be the length of the longest jump made in generating  $J_{i_0, k_0}$ . Such a jump can only be made from a number that is divisible by  $2^M$  (and by no higher power of 2). Thus we must have  $M < i_0$ , since otherwise a number divisible by  $2^{i_0}$  is visited before  $2^{i_0}k_0$  is reached, contradicting the definition of  $k_0$ .

Let  $2^{m+1}$  be the length of the jump when the frog jumps over  $2^{i_0}$ . If this jump starts at  $2^m(2t - 1)$  for some positive integer  $t$ , then it will end at  $2^m(2t - 1) + 2^{m+1} = 2^m(2t + 1)$ . Since it goes over  $2^{i_0}$  we see  $2^m(2t - 1) < 2^{i_0} < 2^m(2t + 1)$  or  $(2^{i_0-m} - 1)/2 < t < (2^{i_0-m} + 1)/2$ . Thus  $t = 2^{i_0-m-1}$  and the jump over  $2^{i_0}$  is from  $2^m(2^{i_0-m} - 1) = 2^{i_0} - 2^m$  to  $2^m(2^{i_0-m} + 1) = 2^{i_0} + 2^m$ .

Considering the jumps that generate  $J_{i_0, k_0}$ , let  $N_1$  be the number of jumps from 1 to  $2^{i_0} + 2^m$ , and let  $N_2$  be the number of jumps from  $2^{i_0} + 2^m$  to  $2^{i_0}k_0$ . By definition of  $i_0$ , it follows that  $2^m$  can be reached from 1 in less than  $N_1$  jumps. On the other hand, because  $m < i_0$ , the number  $2^{i_0}(k_0 - 1)$  can be reached from  $2^m$  in exactly  $N_2$  jumps by using the same jump length sequence as in jumping from  $2^m + 2^{i_0}$  to  $2^{i_0}k_0 = 2^{i_0}(k_0 - 1) + 2^{i_0}$ . The key point here is that the shift by  $2^{i_0}$  does not affect any of divisibility conditions needed to make jumps of the same length. In particular, with the exception of the last entry,  $2^{i_0}k_0$ , all of the elements of  $J_{i_0, k_0}$  are of the form  $2^p(2t + 1)$  with  $p < i_0$ , again because of the definition of  $k_0$ . Because  $2^p(2t + 1) - 2^{i_0} = 2^p(2t - 2^{i_0-p} + 1)$  and the number  $2t - 2^{i_0-p} + 1$  is odd, a jump of size  $2^{p+1}$  can be made from  $2^p(2t + 1) - 2^{i_0}$  just as it can be made from  $2^p(2t + 1)$ .

Thus the frog can reach  $2^m$  from 1 in less than  $N_1$  jumps, and can then reach  $2^{i_0}(k_0 - 1)$  from  $2^m$  in  $N_2$  jumps. Hence the frog can reach  $2^{i_0}(k_0 - 1)$  from 1 in less than  $N_1 + N_2$  jumps, that is, in fewer jumps than needed to get to  $2^{i_0}k_0$  and hence in fewer jumps than required to get to  $2^{i_0}$ . This contradicts the definition of  $k_0$ .

**Second Solution.** Suppose  $x_0 = 1, x_1, \dots, x_t = 2^i k$  are the integers visited by the frog on his trip from 1 to  $2^i k$ ,  $k \geq 2$ . Let  $s_j = x_j - x_{j-1}$  be the jump sizes. Define a reduced path  $y_j$  inductively by

$$y_j = \begin{cases} y_{j-1} + s_j & \text{if } y_{j-1} + s_j \leq 2^i, \\ y_{j-1} & \text{otherwise.} \end{cases}$$

Say a jump  $s_j$  is deleted in the second case. We will show that the distinct integers among the  $y_j$  give a shorter path from 1 to  $2^i$ . Clearly  $y_j \leq 2^i$  for all  $j$ . Suppose  $2^i - 2^{r+1} < y_j \leq 2^i - 2^r$  for some  $0 \leq r \leq i - 1$ . Then every deleted jump before  $y_j$  must

have length greater than  $2^r$ , hence must be a multiple of  $2^{r+1}$ . Thus  $y_j \equiv x_j \pmod{2^{r+1}}$ . If  $y_{j+1} > y_j$ , then either  $s_{j+1} = 1$  (in which case this is a valid jump) or  $s_{j+1}/2 = 2^m$  is the exact power of 2 dividing  $x_j$ . In the second case, since  $2^r \geq s_{j+1} > 2^m$ , the congruence says  $2^m$  is also the exact power of 2 dividing  $y_j$ , thus again this is a valid jump. Thus the distinct  $y_j$  form a valid path for the frog. If  $j = t$  the congruence gives  $y_t \equiv x_t \equiv 0 \pmod{2^{r+1}}$ , but this is impossible for  $2^i - 2^{r+1} < y_t \leq 2^i - 2^r$ . Hence we see  $y_t = 2^i$ , that is, the reduced path ends at  $2^i$ . Finally since the reduced path ends at  $2^i < 2^i k$  at least one jump must have been deleted and it is strictly shorter than the original path.

This problem was proposed by Zoran Sunik.

6. Let  $ABCD$  be a quadrilateral, and let  $E$  and  $F$  be points on sides  $AD$  and  $BC$ , respectively, such that  $AE/ED = BF/FC$ . Ray  $FE$  meets rays  $BA$  and  $CD$  at  $S$  and  $T$ , respectively. Prove that the circumcircles of triangles  $SAE$ ,  $SBF$ ,  $TCF$ , and  $TDE$  pass through a common point.

**First Solution.** Let  $P$  be the second intersection of the circumcircles of triangles  $TCF$  and  $TDE$ . Because the quadrilateral  $PEDT$  is cyclic,  $\angle PET = \angle PDT$ , or

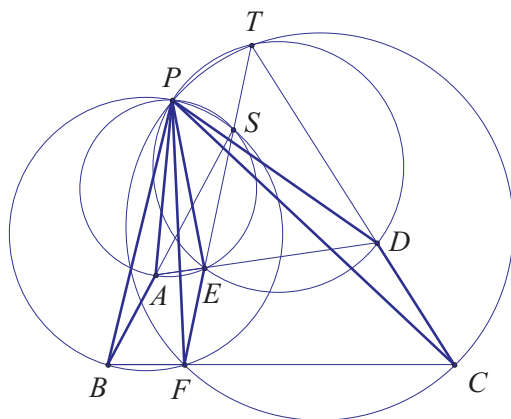
$$\angle PEF = \angle PDC. \quad (*)$$

Because the quadrilateral  $PFCT$  is cyclic,

$$\angle PFE = \angle PFT = \angle PCT = \angle PCD. \quad (**)$$

By equations (\*) and (\*\*), it follows that triangle  $PEF$  is similar to triangle  $PDC$ . Hence  $\angle FPE = \angle CPD$  and  $PF/PE = PC/PD$ . Note also that  $\angle FPC = \angle FPE + \angle EPC = \angle CPD + \angle EPC = \angle EPD$ . Thus, triangle  $EPD$  is similar to triangle  $FPC$ . Another way to say this is that there is a spiral similarity centered at  $P$  that sends triangle  $PFE$  to triangle  $PCD$ , which implies that there is also a spiral similarity, centered at  $P$ , that sends triangle  $PFC$  to triangle  $PED$ , and vice versa. In terms of complex numbers, this amounts to saying that

$$\frac{D - P}{E - P} = \frac{C - P}{F - P} \implies \frac{E - P}{F - P} = \frac{D - P}{C - P}.$$



Because  $AE/ED = BF/FC$ , points  $A$  and  $B$  are obtained by extending corresponding segments of two similar triangles  $PED$  and  $PFC$ , namely,  $DE$  and  $CF$ , by the identical proportion. We conclude that triangle  $PDA$  is similar to triangle  $PCB$ , implying that triangle  $PAE$  is similar to triangle  $PBF$ . Therefore, as shown before, we can establish the similarity between triangles  $PBA$  and  $PFE$ , implying that

$$\angle PBS = \angle PBA = \angle PFE = \angle PFS \quad \text{and} \quad \angle PAB = \angle PEF.$$

The first equation above shows that  $PBFS$  is cyclic. The second equation shows that  $\angle PAS = 180^\circ - \angle BAP = 180^\circ - \angle FEP = \angle PES$ ; that is,  $PAES$  is cyclic. We conclude that the circumcircles of triangles  $SAE$ ,  $SBF$ ,  $TCF$ , and  $TDE$  pass through point  $P$ .

**Note.** There are two spiral similarities that send segment  $EF$  to segment  $CD$ . One of them sends  $E$  and  $F$  to  $D$  and  $C$ , respectively; the point  $P$  is the center of this spiral similarity. The other sends  $E$  and  $F$  to  $C$  and  $D$ , respectively; the center of this spiral similarity is the second intersection (other than  $T$ ) of the circumcircles of triangles  $TFD$  and  $TEC$ .

**Second Solution.** We will give a solution using complex coordinates. The first step is the following lemma.

**Lemma.** *Suppose  $s$  and  $t$  are real numbers and  $x$ ,  $y$  and  $z$  are complex. The circle in the complex plane passing through  $x$ ,  $x + ty$  and  $x + (s + t)z$  also passes through the point  $x + syz/(y - z)$ , independent of  $t$ .*

*Proof.* Four points  $z_1$ ,  $z_2$ ,  $z_3$  and  $z_4$  in the complex plane lie on a circle if and only if the

cross-ratio

$$cr(z_1, z_2, z_3, z_4) = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_4)(z_2 - z_3)}$$

is real. Since we compute

$$cr(x, x + ty, x + (s + t)z, x + syz/(y - z)) = \frac{s + t}{s}$$

the given points are on a circle. □

Lay down complex coordinates with  $S = 0$  and  $E$  and  $F$  on the positive real axis. Then there are real  $r_1, r_2$  and  $R$  with  $B = r_1A$ ,  $F = r_2E$  and  $D = E + R(A - E)$  and hence  $AE/ED = BF/FC$  gives

$$C = F + R(B - F) = r_2(1 - R)E + r_1RA.$$

The line  $CD$  consists of all points of the form  $sC + (1 - s)D$  for real  $s$ . Since  $T$  lies on this line and has zero imaginary part, we see from  $\text{Im}(sC + (1 - s)D) = (sr_1R + (1 - s)R)\text{Im}(A)$  that it corresponds to  $s = -1/(r_1 - 1)$ . Thus

$$T = \frac{r_1D - C}{r_1 - 1} = \frac{(r_2 - r_1)(R - 1)E}{r_1 - 1}.$$

Apply the lemma with  $x = E$ ,  $y = A - E$ ,  $z = (r_2 - r_1)E/(r_1 - 1)$ , and  $s = (r_2 - 1)(r_1 - r_2)$ . Setting  $t = 1$  gives

$$(x, x + y, x + (s + 1)z) = (E, A, S = 0)$$

and setting  $t = R$  gives

$$(x, x + Ry, x + (s + R)z) = (E, D, T).$$

Therefore the circumcircles to  $SAE$  and  $TDE$  meet at

$$x + \frac{syx}{y - z} = \frac{AE(r_1 - r_2)}{(1 - r_1)E - (1 - r_2)A} = \frac{AF - BE}{A + F - B - E}.$$

This last expression is invariant under simultaneously interchanging  $A$  and  $B$  and interchanging  $E$  and  $F$ . Therefore it is also the intersection of the circumcircles of  $SBF$  and  $TCF$ .

This problem was proposed by Zuming Feng.