XIII. International Dürer Competition

solutions

20 November 2020

E+

E+1. Determine all triples of positive integers a, b, c that satisfy
a) $[a, b] + [a, c] + [b, c] = [a, b, c]$.
b) $[a, b] + [a, c] + [b, c] = [a, b, c] + (a, b, c)$.
Remark: Here $[x, y]$ denotes the least common multiple of positive integers x and y, and (x, y) denotes their greatest common divisor.

First solution: a) We will show that there are no solutions. Observe that if p^k $(p, k \in Z^+)$ is a prime power that divides all three numbers, then if we divide the numbers by p^k, the equality still remains true, as all terms get divided by p^k. If we do this with all prime powers appearing in the prime factorization of the GCD $d = (a, b, c)$, then in the end we will have $(a, b, c) = 1$ and the equation will still hold. So in the remaining part of the solution we will assume $(a, b, c) = 1$.

Take a prime p that divides at least one of a, b and c. The equation is symmetric in the three variables so we can assume $p \mid a$. Then p divides $[a, b]$, $[a, c]$ and $[a, b, c]$ too, so by the equation it also divides $[b, c]$. So it divides either b or c (but not both, as otherwise $(a, b, c) = 1$ would not hold). So every prime divisor of a, b or c divides exactly two of the numbers.

Moreover, it is also true that if p divides both a and b, then it actually appears in the prime factorizations of a and b to the same power. We will prove this by contradiction. Suppose that p appears to the k-th power in a and to the l-th power in b, and WLOG suppose $k > l$. Then let us compute the p-power appearing in each of the terms of the equation: $[a, b]$, $[a, c]$ and $[a, b, c]$ all have p^k and $[b, c]$ has p^l (using the fact that p does not divide c). So any prime appears in the factorizations of two of the numbers, and it appears in both to the same power.

If we group all primes appearing in a, b or c depending on which two of the numbers they divide, we can write the numbers in the following form: $a = de$, $b = ef$ and $c = fd$, where d, e and f are pairwise coprime. (For example e is the product of prime powers dividing both a and b.) Then $[a, b] + [a, c] + [b, c] = def + def + def = 3def$, and $[a, b, c] = def$. But this is impossible since d, e and f are positive. So there are no solutions.

b) Again observe that if a prime divides all three numbers then we can again divide all three numbers by it, and the equation remains true. So for the moment, let us only consider the cases where we have $d = (a, b, c) = 1$.

Take a prime p that divides at least two numbers out of the three. By symmetry we can assume that p divides a and b. Then it will divide all of $[a, b]$, $[a, c]$, $[b, c]$ and $[a, b, c]$, so by the equation it must also divide (a, b, c). However $(a, b, c) = 1$ so this is impossible. So any prime can only divide at most one of the three numbers, so the three numbers are pairwise coprime. So the equation will be the following: $ab + ac + bc = abc + 1$.

By symmetry, we can assume that a is the smallest of the three numbers (it is not necessarily distinct from the other two, as there can be multiple smallest numbers). Consider three cases according to the possible values of a:

- If $a = 1$ then $b + c + bc = bc + 1$, so $b + c = 1$ which is impossible.
- If $a \geq 3$ then $ab + ac + bc \leq \frac{abc}{3} + \frac{abc}{3} + \frac{abc}{3} < abc + 1$, which is also impossible.
- Finally if $a = 2$ then $2b + 2c + bc = 2bc + 1$, which after reordering gives $bc - 2b - 2c + 1 = 0$, so $(b - 2)(c - 2) = 3$. As b and c are positive integers, the only possible solution is $a = 2$, $b = 3$ and $c = 5$.

So up to reordering of the variables, the only solution with $(a, b, c) = 1$ is $a = 2$, $b = 3$ and $c = 5$, and we can check that this is indeed a solution.

Now let us turn to the cases where $d = (a, b, c) > 1$. As dividing everything by d gives a good solution where the GCD of the three numbers is 1, the original numbers must be (up to reordering) of

the form $a = 2d$, $b = 3d$ and $c = 5d$ for some positive integer d. We can check that these are all correct solutions indeed, as $[a, b] + [a, c] + [b, c] = 6d + 10d + 15d = 31d$ and $[a, b, c] + (a, b, c) = 30d + d = 31d$ too.

Second solution: a) We know that $[a, b] \mid [a, b, c]$ and similarly $[b, c]$ and $[c, a]$ also divide $[a, b, c]$. So there exist positive integers p, q and r such that $[a, b, c] = p[a, b] = q[b, c] = r[c, a]$. Divide the equation in the problem by $[a, b, c]$ to get

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$$

The positive integer solutions of this equation (up to reordering) are $(2, 3, 6)$, $(2, 4, 4)$ and $(3, 3, 3)$.

Here is a possible way to derive this: suppose WLOG that $p \le q \le r$. If $p = 1$, the LHS would be greater than 1 so this is impossible. If $p > 3$ then the LHS is at most $\frac{3}{4}$ so this is also impossible. If $p = 3$ then the LHS can only be 1 if $p = q = r = 3$, which is indeed a solution. Finally if $p = 2$ then we have $\frac{1}{q} + \frac{1}{r} = \frac{1}{2}$. Reordering this, we get $2r + 2q = qr$ so $qr - 2r - 2q + 4 = 4$, and this factorizes as $(q - 2)(r - 2) = 4$. This gives two possible solutions for q and r: $(q, r) = (3, 6)$ and $(q, r) = (4, 4)$.

Now note that if p, q and r are not pairwise coprime, then we can reach a contradiction: assume that a prime d divides both p and q. Then $d \mid \frac{[a,b,c]}{[a,b]}$ means that d appears in c to a higher power than in a, and $d \mid \frac{[a,b,c]}{[b,c]}$ means that d appears in a to a higher power than in c. And this is impossible.

So p, q and r must be pairwise coprime, but none of the solutions $(2, 3, 6)$, $(2, 4, 4)$ or $(3, 3, 3)$ satisfy this. So there is no solution to the original equation.

b) Let us start similarly to part **a)**: as $(a, b, c) \mid [a, b, c]$, we have a positive integer s with $[a, b, c] = s(a, b, c)$. Also observe that (a, b, c) divides the pairwise LCM's of the three numbers (e.g. $(a, b, c) \mid a \mid [a, b]$), so if we define p, q and r in the same way as above, then p, q and r will all be divisors of s. Rearranging the equation and dividing by $[a, b, c]$ now gives

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - \frac{1}{s} = 1$$

As the equation is still symmetric in a, b and c, we can assume that $p \le q \le r$.

If $p = 1$ then as $r \mid s$, we have $r \le s$ so $\frac{1}{r} - \frac{1}{s} \ge 0$, so since $\frac{1}{q} > 0$, the LHS is greater than 1, a contradiction.

If $p \ge 3$, then $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - \frac{1}{s} < 3 \cdot \frac{1}{3} + 0$, so the LHS is smaller than 1.

So we must have $p = 2$. This yields

$$\frac{1}{q} + \frac{1}{r} - \frac{1}{s} = \frac{1}{2}$$

Suppose $q = 2$. Then we get $\frac{1}{r} - \frac{1}{s} = 0$, so $r = s$. This means $(a, b, c) = [c, a]$, so as $(a, b, c) \le a \le [c, a]$, we have $(a, b, c) = a = [c, a]$. This gives $a = c$. Then it is easy to see that the original equation reduces to $[a, b] + a = (a, b)$, which is impossible as $[a, b] + a > a \ge (a, b)$.

Suppose $q \ge 4$. Then $\frac{1}{q} + \frac{1}{r} - \frac{1}{s} < 2 \cdot \frac{1}{4} + 0 = \frac{1}{2}$, again a contradiction.

So we must have $q = 3$. Then we get

$$\frac{1}{r} - \frac{1}{s} = \frac{1}{6}$$

Here $r \ge q = 3$, and also $r \le 5$, since $r \ge 6$ would mean that $\frac{1}{r} - \frac{1}{s} < \frac{1}{6}$. So $r \in \{3, 4, 5\}$, and in each case s can be determined. We get the following three possibilities for the quadruple p, q, r, s:

$$(p; q; r; s) \in (2; 3; 3; 6), (2; 3; 4; 12), (2; 3; 5; 30)$$

The observation in part **a)** that p, q and r are pairwise coprime is true in this case as well, so this only leaves the case $(p;q;r;s)=(2;3;5;30)$. This means

$$[a,b,c]=2[a,b]=3[b,c]=5[c,a]=30(a,b,c)$$

So $[a,b,c]=2[a,b]$ means that the exponent of the prime 2 in c is higher than in both a and b. So in $[a,b,c]$, 2 appears to a higher power than in (a,b,c). Similarly 3 and 5 also appear to a higher power in $[a,b,c]$ than in (a,b,c). So $\frac{[a,b,c]}{(a,b,c)}\geq 2\cdot 3\cdot 5=30$.

Since we have equality here, the only possible case is that the powers of 2 in a and b are the same, and the power of 2 in c is one larger than that. The analogue is true for powers of 3 and 5 too (but of course they have to be the largest in b and a respectively). Also every prime appearing in $[a,b,c]$ other than 2, 3 or 5 has to appear in (a,b,c) to an equal power as in $[a,b,c]$. So these primes appear in all of a, b and c to the same power.

To summarize, we have $a=2^x3^y5^{z+1}k$, $b=2^x3^{y+1}5^zk$ and $c=2^{x+1}3^y5^zk$ for some natural numbers $x,y,z\geq 0$ and a positive integer k that is coprime to 2, 3 and 5.

Taking out the common term $d=2^x3^y5^zk$, this means that $a=5d$, $b=3d$ and $c=2d$ where d can be any positive integer.

So the solution is that up to reordering, $(a;b;c)=(5d;3d;2d)$ where d is an arbitrary positive integer. In the original equation we can check that these are indeed solutions: $15d+10d+6d=30d+d$.

E+2. 21 bandits live in the city of Warmridge, each of them having some enemies among the others. Initially each bandit has 240 bullets, and duels with all of his enemies. Every bandit distributes his bullets evenly between his enemies, this means that he takes the same number of bullets to each of his duels, and uses each of his bullets only in one duel. In case the number of his bullets is not divisible by the number of his enemies, he takes as many bullets to each duel as possible, but takes the same number of bullets to every duel, so it is possible that in the end some bullets will remain by the bandit.
Shooting is banned in the city, therefore a duel consists only of comparing the number of bullets in the guns of the opponents, and the winner is the one who has more bullets. After the duel the sheriff takes the bullets of the winner to himself and as a protest the loser shoots all of his bullets into the air. What is the largest possible number of bullets by the sheriff after all of the duels have ended?
The enemy relations are mutual. If two opponents have the same number of bullets in their guns during a duel, then the sheriff takes the bullets of the bandit who has the wider hat among them.
Example: If a bandit has 13 enemies then he takes 18 bullets with himself to each duel, and 6 bullets remain by him in the end.

First solution: If there is one main villain, who is the enemy of everyone else, and the others are all friends with each other, then there are 20 duels in total, and to each of them the winner has taken all of his bullets with himself, so in this case the sheriff has $20 \cdot 240 = 4800$ bullets in the end.

We claim that it is not possible that the sheriff has a larger number of bullets by himself after the duels. Consider the bandit who brings the least amout of bullets to his duels, if there are more bandits with this property then we consider the bandit who has the narrowest hat among them. This bandit looses each of his duels, so none of his 240 bullets end up by the sheriff. The other bandits have $20 \cdot 240 = 4800$ bullets in total, so the sheriff cannot take more than 4800 bullets to himself.

Second solution: We get the lower bound $20 \cdot 240$ in the same way as in the first solution.

Let us rewrite this exercise as a graph theory problem. We define a graph G, in which the vertices correspond to the bandits, and there is an edge between two bandits if and only if they are enemies. The bandit V brings at most $\frac{240}{d_V}$ bullets to a duel, where d_V denotes the number of the enemies of V. Translating it to the graph theoretic point of view, d_V is the degree of the vertex corresponding to bandit V in G. On the uv edge the sheriff can take at most $\max\left(\frac{240}{d_v}, \frac{240}{d_u}\right)$ bullets, therefore the following can be proven:

$$\sum \max\left(\frac{240}{d_v}, \frac{240}{d_u}\right) \leq 20 \cdot 240$$

where we take the sum over all edges in G.

Let us divide the above statement by 240 and generalise the statement we want to prove for an arbitrary graph $G = (V, E)$:

$$\sum_{uv \in E} \max\left(\frac{1}{d_v}, \frac{1}{d_u}\right) \leq |V| - 1$$

We are going to prove this generalised statement. It is clear that it is enough to prove the statement for connected graphs.

Let Δ denote the maximum degree in G. It is clear, that $\Delta \leq |E|$, and $\max\left(\frac{1}{d_v}, \frac{1}{d_u}\right) \leq \frac{1}{d_u} + \frac{1}{d_v} - \frac{1}{\Delta}$, thus

$$\sum_{uv \in E} \max\left(\frac{1}{d_v}, \frac{1}{d_u}\right) \leq \sum_{uv \in E} \left(\frac{1}{d_u} + \frac{1}{d_v} - \frac{1}{\Delta}\right) = |V| - \frac{|E|}{\Delta} \leq |V| - 1$$

The equality in the middle is satisfied, because every vertex u is by definition the endpoint of exactly d_u edges, hence it will appear d_u times in the sum.

Our estimate also shows that equality is only possible in the case when $|E| = \Delta$ holds, i.e. only in the case of a star graph (one of the vertices is connected with every other vertex by an edge, and the graph has no more edges), and it is clear that in this case there is really an equality.

Third solution, sketch: Here we are providing a different proof for the more general graph theoretic inequality from the previous solution.

Let u be an arbitrary edge of the graph G, d_u its degree and e an edge which is incident to u. Let us consider a random spanning tree of G, we choose each of the spanning trees with equal probability. Then the probability that e is contained in this randomly chosen spanning tree is at least $\frac{1}{d_u}$. This is a nice statement, and we leave proof of it as an exercise to the reader. The statement implies that every uv edge is at least with $\max\left(\frac{1}{d_v}, \frac{1}{d_u}\right)$ probability in the randomly chosen spanning tree. Let $\mathbb{I}_{uv}$ denote the indicator function of the event that uv is contained in the spanning tree, i.e. it takes the value 1 if uv is contained in the spanning tree, and 0 if it is not. The expected value of $\mathbb{I}_{uv}$ is equal to the probability that the edge is contained in the spanning tree. It is known that the expected value is linear, therefore

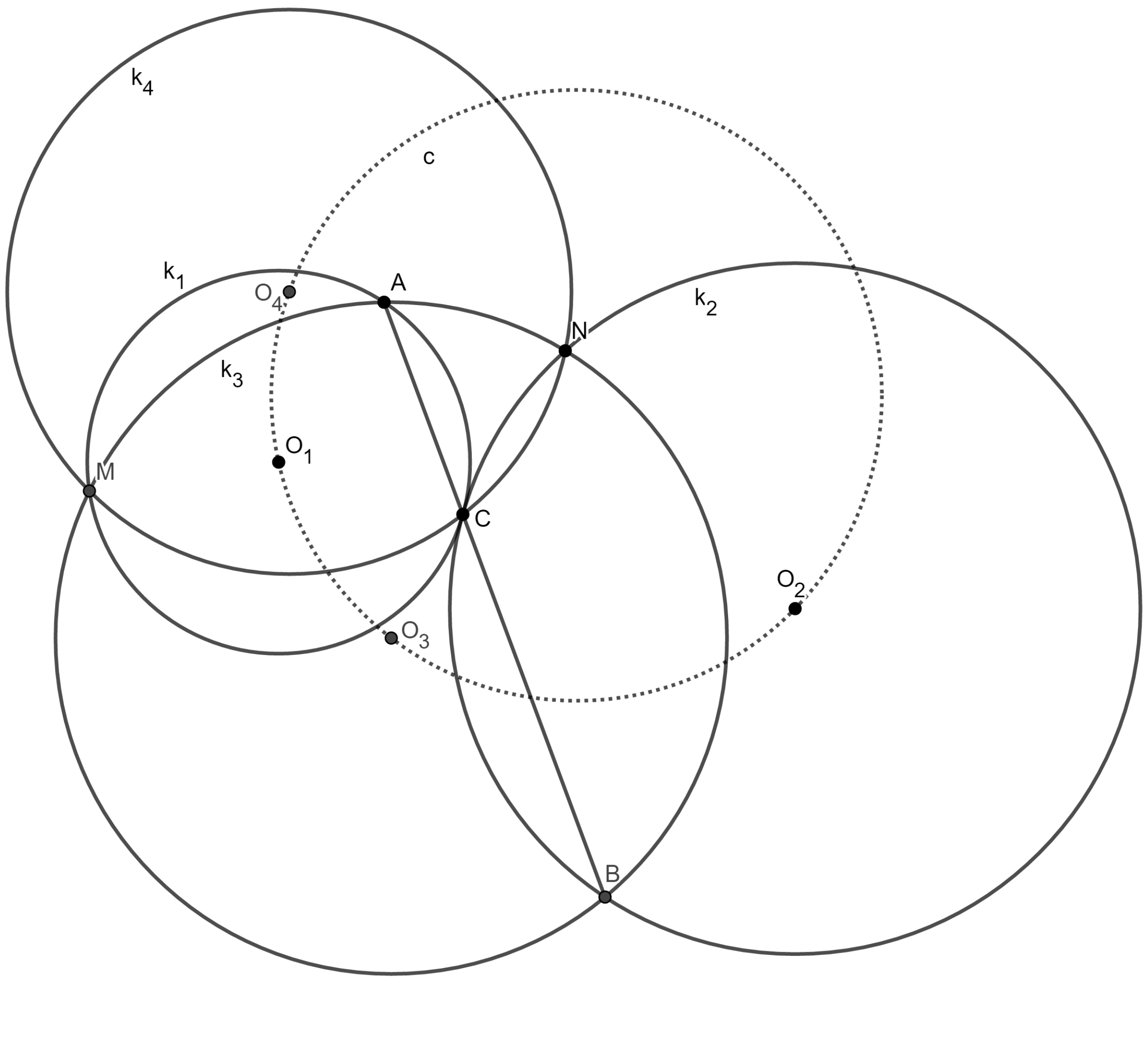
$$\sum_{uv\in E} \max\left(\frac{1}{d_v}, \frac{1}{d_u}\right) \le \sum_{uv\in E} \mathbb{E}(\mathbb{I}_{uv}) = \mathbb{E}\left(\sum_{uv\in E} \mathbb{I}_{uv}\right) = |V| - 1$$

, where the last equality is satisfied because the expected value of the sum of the indicator functions tells us exactly the expected number of edges of the spanning tree.

E+3. Let k_1 and k_2 be two circles that are externally tangent at point C. We have a point A on k_1 and a point B on k_2 such that C is an interior point of segment AB. Let k_3 be a circle that passes through points A and B and intersects circles k_1 and k_2 another time at points M and N respectively. Let k_4 be the circumscribed circle of triangle CMN. Prove that the centres of circles k_1, k_2, k_3 and k_4 all lie on the same circle.

Solution: The main observation is that the line connecting the intersection points of two circles is perpendicular to the line through their centers. We are going to use angle chasing (working with directed angles modulo π) to solve the problem.

Let O_1, O_2, O_3, O_4 be the centers of the circles k_1, k_2, k_3, k_4, respectively. $O_1O_4 \perp MC$, since the circles k_1 and k_4 intersect at points M and C. Similarly, $O_1O_3 \perp AM$, hence $\sphericalangle O_3O_1O_4 = \sphericalangle AMC$. Analogously, $O_2O_3 \perp BN$ and $O_4O_2 \perp CN$, so $\sphericalangle O_3O_2O_4 = \sphericalangle BNC$. k_1 is tangent to k_2, hence $\sphericalangle AMC = \sphericalangle BNC$. (This is because if we let X be a point on the common internal tangent of k_1 and k_2, then $\sphericalangle AMC = \sphericalangle ACX = \sphericalangle BCX = \sphericalangle BNC$ using the inscribed angle theorem.) Comparing this against our previous results, have $\sphericalangle O_3O_1O_4 = \sphericalangle O_3O_2O_4$, whence the points O_1, O_2, O_3, O_4 are concyclic, as required.



E+4. Let p and q be polynomials with integer coefficients such that p is of degree n and has n nonnegative real roots (counted with multiplicity). Find all pairs of polynomials (p, q) that satisfy the equation

$$p(x^2) + q(x^2) = p(x)q(x)$$

and also the conditions mentioned above.

Solution: Let k be the degree of q. Then $p(x)q(x)$ has degree $n + k$.

If $k > n$, then $p(x^2) + q(x^2)$ has degree $2k \neq n + k$. If $k < n$, then $p(x^2) + q(x^2)$ has degree $2n \neq n + k$.

The only possibility is therefore that the degree of q is also n.

Let a be the leading coefficient of p and b the leading coefficient of q. Then $p(x)q(x) = p(x^2)+q(x^2)$ has leading coefficient $ab = a + b$.

So $ab - a - b = 0$, i.e. $(a - 1)(b - 1) = 1$. Since a and b are non-zero integers, this is only possible if $a = b = 2$.

If 0 is a root of multiplicity r in $p(x)$, and a root of multiplicity s in $q(x)$, then it is a root of multiplicity $r + s$ in $p(x)q(x)$.

If $r < s$, then $p(x^2)+q(x^2)$ is divisible by x^{2r}, but not divisible by any greater power of x. $2r \neq r+s$.

Similarly, if $s < r$, then $p(x^2) + q(x^2)$ is divisible by x^{2s}, but not divisible by any higher power of x. $2s \neq r + s$.

Therefore equality is only possible if $r = s$.

Let $p(x) = x^r P(x)$ and $q(x) = x^r Q(x)$, where 0 is neither a root of P nor a root of Q.

Then $x^{2r}P(x)Q(x) = x^{2r}(P(x^2) + Q(x^2))$, and so $P(x)Q(x) = P(x^2) + Q(x^2)$.

It is still true that P and Q have both degree m, and both have leading coefficient 2.

$p(x)$ had only non-negative real roots, hence the roots of $P(x)$ are positive real numbers.

Since $P(x^2) + Q(x^2)$ is an even function, $P(x)Q(x)$ is also even, thus if x is a root, then the same is true for $-x$.

This implies that if we multiply the positive roots of $P(x)$ by -1 we get again roots of $P(x)Q(x)$, and because they are not positive, they cannot be roots of $P(x)$, only of $Q(x)$.

So if $P(x) = 2(x - r_1)(x - r_2)\dots(x - r_m)$, then $Q(x) = 2(x + r_1)(x + r_2)\dots(x + r_m)$.

Therefore $P(x)Q(x) = 4(x^2 - r_1^2)(x^2 - r_2^2)\dots(x^2 - r_m^2) = 2(x^2 - r_1)(x^2 - r_2)\dots(x^2 - r_m) + 2(x^2 + r_1)(x^2 + r_2)\dots(x^2 + r_m)$

Denoting x^2 by y we get that

$4(y - r_1^2)(y - r_2^2)\dots(y - r_m^2) = 2(y - r_1)(y - r_2)\dots(y - r_m) + 2(y - r_1)(y - r_2)\dots(y - r_m)$.

Let us assume that P is not a constant polynomial.

The constant term of P is an integer, which is non-zero because 0 is not contained between the roots anymore. So the absolute value of the constant term is at least 1.

The constant term is the product of the roots with some sign, so either every root r_i has absolute value 1, or there is a root among them with absolute value greater than 1.

We know that the roots r_i are all positive, so they are either all equal to 1, or the biggest root among them (which we will denote by r_m) is greater than 1.

If every $r_i = 1$, then $4(y-1)^m = 2(y-1)^m+2(y+1)^m$, so $(y-1)^m = (y+1)^m$, which is impossible.

If r_m is the biggest root and $r_m > 1$, then in case of $y = r_m^2$, $4(y - r_1^2)(y - r_2^2)\dots(y - r_m^2) = 0$.

However $r_m^2 > r_m \geq r_i$ for every i, hence $2(y - r_1)(y - r_2)\dots(y - r_m)$ is a product of positive terms for $y = r_m^2$, and naturally $2(y + r_1)(y + r_2)\dots(y + r_m)$ is also a product of positive numbers for $y = r_m^2$.

Hence $2(y - r_1)(y - r_2)\dots(y - r_m) + 2(y + r_1)(y + r_2)\dots(y + r_m)$ is positive for $y = r_m^2$.

So $4(y - r_1^2)(y - r_2^2)\dots(y - r_m^2) \neq 2(y - r_1)(y - r_2)\dots(y - r_m) + 2(y + r_1)(y + r_2)\dots(y + r_m)$.

We get that the only remaining possibility is that P and Q are constant functions. We have already shown that the leading coefficient is 2, thus $P(x)$ and $Q(x)$ are both the constant polynomial 2.

Therefore the solution can only have the form $p(x) = 2x^n, q(x) = 2x^n$. This gives indeed a good solution, because $p(x)$ has n non-negative real roots and $p(x)q(x) = 4x^{2n} = p(x^2) + q(x^2)$.

E+5. We have n distinct lines in three-dimensional space such that no two lines are parallel and no three lines meet at one point. What is the maximal possible number of planes determined by these n lines?
We say that a plane is determined if it contains at least two of the lines.

Solution: For even n: $\frac{n^2}{4}$, for odd n: $\frac{(n-1)(n+1)}{4}$, so in general $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil$.

Upper bound: Consider n given lines in the three-dimensional space, such that no 2 of them are parallel and no 3 of them are concurrent. Consider the graph G, whose vertices are the lines, and for every plane determined by two of the n lines we create exactly one edge between two of the lines, which determine this plane. This way the graph will have exactly as many edges as there are determined planes. We claim that G is triangle-free.

Let's use proof by contradiction. Assume G has a triangle in it, that is, there are 3 distinct lines e_1, e_2 and e_3 and 3 distinct planes s_1, s_2 and s_3 such that e_1 and e_2 determine s_3, e_1 and e_3 determine s_2, e_2 and e_3 determine s_1. As there are no parallel lines, two lines determine a plane if and only if they intersect, thus e_1, e_2 and e_3 are pairwise intersecting. Since they are not concurrent, this is only possible if they form a triangle, but then they lie on one plane, so s_1, s_2 and s_3 can't be distinct planes which is a contradiction.

Thus G really is triangle-free, so according to Turán's theorem it can have at most $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil$ edges, that is, this is the maximal number of planes n lines can determine, and this is what we wanted to prove.

Lower bound: We have to give a construction with n lines, which determine $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil$ planes. We know that equality in Turán's theorem occurs when the n lines are divided into two almost equal groups, so we have to look for such a construction, where two lines intersect if and only if they are in a different group. The idea is to look for lines of the following form:
Let one of the groups have lines whose orthogonal projection onto the xy plane is parallel to the x axis, namely let e_k's projection's equation be $y = k$ where $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$. Likewise, let the other group have lines f_k whose orthogonal projection to the xy plane has equations $x = k$ for all $1 \leq k \leq \lceil \frac{n}{2} \rceil$. After this, we want to set the slope of these lines with respect to the xy plane such that the e lines have pairwise different slopes, the f lines also have pairwise different slopes, and any two e_i and f_j should intersect. Luckily, we can achieve this:

For all $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$ let e_k's equations be $y = k$ and $z = kx$. Likewise, for all $1 \leq k \leq \lceil \frac{n}{2} \rceil$ let f_k's equations be $x = k$ and $z = ky$. Then for arbitrary $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$, $1 \leq j \leq \lceil \frac{n}{2} \rceil$ both e_i and f_j passes through the point (j, i, ij), as this point satisfies both lines' equations. It's clear that these intersection points are different for different pairs of lines, so there are no 3 lines which are concurrent. As we chose the slopes of the lines to be different there can't be any parallel lines either. Hence this really is a correct construction for n lines which determine $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil$ planes.

Remark: A construction can also be given using a hyperboloid of revolution.