

1 (a) *Saint-Peterburg, 1998* Let $d(n)$ denote the number of positive divisors of the
 PEN J11 number n . Prove that the sequence $d(n^2+1)$ does not become strictly monotonic from some point onwards.

(b) Prove that $d((n^2+1)^2)$ does not become monotonic from any given point onwards.

Solution for (a). Intuitively, the sequence being required to be strictly monotonic points that it will eventually grow rather *fast*. This is a hint to the solution. Note that if n is even, then the set of divisors of n^2+1 can be partitioned into pairs $\left\{d, \frac{n^2+1}{d}\right\}$, where $d < \frac{n^2+1}{d}$. Clearly d is odd and less than n . Hence we have at most $\frac{n}{2}$ pairs, consequently $d(n^2+1) \leq n$.

Assuming to the contrary that the sequence becomes strictly monotonic starting with an N , it's obvious that it must be increasing (otherwise $d(n^2+1)$ would be forced to take negative values from some point $n > N$ onwards). Note that since n^2+1 is not a perfect square for any $n > 0$, hence $d(n^2+1)$ is an even number for every positive integer n . Since $d(n^2+1)$ is strictly monotonic for $n \geq N$, we deduce

$$d((n+1)^2+1) \geq d(n^2+1) + 2.$$

A straightforward induction proves that

$$d((n+k)^2+1) \geq d(n^2+1) + 2k.$$

By the inequality established in the beginning of the solution, for $N+t$ even we obtain the inequalities

$$N+t > d((N+t)^2+1) \geq d(N^2+1) + 2t,$$

or

$$N > d(N^2+1) + t$$

for any $t > 0$ which is impossible, since the rest of the terms of the inequality are constant. \square

AFTERTHOUGHTS 1. *It must be mentioned that the problem was proposed for the Elimination Round of Saint-Peterburg Mathematical Olympiad in 1998 for 11th grade. The problem's author is A. Golovanov. Only 2 contestants solved the problem at the contest.*

Solution for (b). Note that since the sequence is not required to be strictly monotonic, we cannot infer that it will grow very fast, so the argument used at (a) fails. We will prove the following generalization:

Claim 1. *Let t and m be two positive integers. Then the sequence $d((n^2+m^2)^t)$ does not become monotonic from any given point onwards.*

Suppose, to the contrary, that from some point onwards, the sequence becomes monotonic. We will firstly show that it must be increasing. Indeed, take a prime p of the form $4k+1$. Clearly -1 is a quadratic residue $(\text{mod } p)$, hence so is $-m^2$, so there is an integer r so that $p|r^2+m^2$. Take now d different primes s_1, \dots, s_d of the form $4u+1$ and let $r_i \in \mathbb{Z}$ so that $s_i | r_i^2+m^2$.

Using the Chinese Remainder Theorem there is an integer N , so that $N \equiv r_i \pmod{s_i}$, for every $i = 1, \dots, d$. Then $N^2 + m^2 \equiv r_i^2 + m^2 \pmod{s_i}$, hence $s_1 \dots s_d | N^2 + m^2$. This implies that $d((N^2 + m^2)^t)$ is unbounded, consequently it must be increasing from some point x_0 onwards.

For shortness of notations let $f_n = f(n) = d((n^2 + m^2)^t)$. We will use the following very simple result.

Lemma 1. $\gcd(a^2 + m^2, (a - 1)^2 + m^2) = 1$ if $\gcd(2a - 1, 4m^2 + 1) = 1$.

Proof of Lemma 1. Let $\gcd(2a - 1, 4m^2 + 1) = 1$ and suppose there is a prime p dividing both $a^2 + m^2$ and $(a - 1)^2 + m^2$. By subtraction, we obtain $p | 2a - 1$. Then $2a \equiv 1 \pmod{p}$, so $4a^2 \equiv 1 \pmod{p}$, or $4a^2 + 4m^2 \equiv 1 + 4m^2 \pmod{p}$. Since $p | 4(a^2 + m^2)$ we obtain $0 \equiv 1 + 4m^2 \pmod{p}$, contradicting $\gcd(2a - 1, 4m^2 + 1) = 1$. \square

Take $x > x_0$ so that $\gcd(2x - 1, 1 + 4m^2) = 1$. Then from Lemma 1 and the identity $[x^2 + m^2][(x - 1)^2 + m^2] = (x^2 - x + m^2)^2 + m^2$ we get the inequality $f_{x-1}f_x \leq f_{x^2-x+m^2}$, since $d(uv) = d(u) \cdot d(v)$ if $\gcd(u, v) = 1$.

We now state the following result, which we are going to use a bit later.

Lemma 2. *Let M be an integer. Then there exists a positive integer λ so that the polynomial $h(x) = 4x^2 - \lambda$ satisfies*

$$\gcd(2h(x) + 1, M) = 1, \forall x \in \mathbb{Z}$$

Proof of Lemma 2. Since $2h(x) + 1$ is odd, we need only prove the lemma for odd M . So assume M is odd and let $\{b_1, \dots, b_s\}$ be the set of prime divisors of M . We are looking for λ so that $b_i \nmid 2h(x) + 1 = 8x^2 - 2\lambda + 1, \forall i = \overline{1, s}$. Since b_i 's are odd, the last condition is equivalent to $b_i \nmid (4x)^2 - (4\lambda - 2)$. It is enough to find a λ so that $4\lambda - 2$ is a quadratic nonresidue $\pmod{b_i}$. For every prime b_i there exists a quadratic non-residue r_i (actually there are $\frac{b_i - 1}{2}$ of them). We will apply once again the Chinese Remainder Theorem in the following way:

We are looking for an integer L satisfying the following system of equations:

$$L \equiv r_i \pmod{b_i}, \forall i = \overline{1, s}$$

$$L \equiv 2 \pmod{4}$$

and take $\lambda = \frac{L - 2}{4}$. Clearly we can assume $\lambda > 0$. \square

Let's continue with the problem. Take $M = 1 + 4m^2$ in Lemma 2 to obtain such λ and $h(x)$. Using the monotonicity of f we deduce the chain of inequalities

$$f_{x-1}^2 \leq f_{x-1}f_x \leq f_{x^2-x+m^2} \leq f_{4(x-1)^2-\lambda},$$

for sufficiently large $x > x_0$. Here, we may also assume that x_0 is sufficiently large so that $x > x_0$ guarantees that $h(x) > x_0$. Note that the inequality $f_{x-1}f_x \leq f_{x^2-x+m^2}$ provides another proof that if f is monotonic, then it must be increasing. Hence $f_q^2 \leq f_{h(q)}$, where $q = x - 1 \geq x_0$, and

$\gcd(2q + 1, 1 + 4m^2) = 1$. Because by Lemma 2 we have $\gcd(2h(q) + 1, 4m^2 + 1) = 1$ we further get $f(q)^4 \leq \{f(h(q))\}^2 \leq f[h(h(q))]$. By an easy induction we obtain the inequalities

$$f(q)^{2^k} \leq f\left(\underbrace{h(h(\dots h(q)\dots))}_{k \text{ times}}\right) \leq f\left[(4q)^{2^k}\right].$$

Here we have iteratively used the fact that $h(z) < 4z^2$. We are going now to summarize the obtained results. Let $c = f(q)$ and define $g(z)$ to be the positive integer satisfying

$$(4q)^{2^{g(z)}} \leq z < (4q)^{2^{g(z)+1}}.$$

We easily obtain $g(z) = \lfloor \log_2 \lfloor \log_{4q} z \rfloor \rfloor$. Then the above inequality and the monotonicity of f implies

$$c^{2^{g(z)}} \leq f(z)$$

for sufficiently large z . With this, we have found a lower estimate for $f(z)$.

Let's find an upper estimate for $f(x)$ which would contradict, for large enough x the lower estimate obtained above. For this, let $(p_i)_{i \geq 1}$ be the sequence of prime numbers, *not containing* the prime divisors of m . Let's take a closer look at $f(p_1 \dots p_k)$. Let $(p_1 \dots p_k)^2 + m^2 = \prod_{i=1}^s q_i^{\alpha_i}$. Using divisibility arguments, we have $q_i > p_j$ for all $i = \overline{1, s}$ and $j = \overline{1, s}$. This clearly implies $\sum_{i=1}^s \alpha_i \leq 2k$. Note that

$$f(p_1 \dots p_k) = d\left(\left[(p_1 \dots p_k)^2 + m^2\right]^t\right) = (t\alpha_1 + 1) \dots (t\alpha_s + 1) =_{\text{def}} h(\alpha_1, \dots, \alpha_s)$$

Using the already stated inequality $\sum_{i=1}^s \alpha_i \leq 2k$ we will prove that $h(\alpha_1, \dots, \alpha_s) \leq (t+1)^{2k}$.

Indeed, note that if $a > 1$ then $(t+1)(t(a-1)+1) \geq ta+1$. Hence if there is some $\alpha_i > 1$, Without Loss Of Generality, $\alpha_1 > 1$, we have $h(\alpha_1, \alpha_2, \dots, \alpha_s) \leq h(\alpha_1 - 1, \alpha_2, \dots, \alpha_s, 1)$. By repeated applications of this inequality until $\alpha_i = 1$, for all i , we obtain the following inequality

$$f(p_1 \dots p_k) = h(\alpha_1, \dots, \alpha_s) \leq h\left(\underbrace{1, 1, \dots, 1}_{\sum \alpha_i}\right) \leq (t+1)^{\sum \alpha_i} \leq (t+1)^{2k} = T^k,$$

where $T = (t+1)^2$. Define now the function $l(x)$ to be equal $v+1$, where v is the unique positive integer for which $p_1 \dots p_v < x \leq p_1 \dots p_{v+1}$. Using once again the monotonicity of f , we establish the following upper bound for the function f :

$$f(x) \leq f(p_1 \dots p_{l(x)}) \leq T^{l(x)}$$

Now, since $g(x) = \lfloor \log_2 \lfloor \log_{4q} x \rfloor \rfloor$, we have $g(x) > \log_2 \lfloor \log_{4q} x \rfloor - 1$, hence

$$2^{g(x)} > 2^{\log_2 \lfloor \log_{4q} x \rfloor - 1} = \frac{1}{2} \lfloor \log_{4q} x \rfloor.$$

It thus follows that

$$T^{l(x)} \geq f(x) \geq c^{2^{\theta(x)}} > \sqrt{c}^{\lfloor \log_{4q} x \rfloor}.$$

By the fact that f is unbounded, we can choose c as large as we want, hence we can assume $\sqrt{c} > T^2$. Then, for reaching a contradiction, we will show that $l(x) < 2\lfloor \log_{4q} x \rfloor$ for large enough x . Since $1 + \log_{4t} x < -2 + 2\log_{4t} x < 2\lfloor \log_{4t} x \rfloor$ for $\log_{4q} x > 3$, it is sufficient to prove $l(x) - 1 < \log_{4q} x$ for large enough x . The last inequality is equivalent to $(4q)^{l(x)-1} < x$. Recall that $4q$ is a constant value. We find that the primes grow very fast so that the inequality $(4q)^{l(x)-1} < p_1 \dots p_{l(x)-1}$ holds for large enough x . By the definition of $l(x)$, we have then, indeed, $p_1 \dots p_{l(x)-1} < x$, obtaining $l(x) - 1 < \log_{4q} x$, what we wanted. □

AFTERTHOUGHTS 2 (About the sequence $\{p_i\}_{i \geq 1}$). *We omitted proof of the validity of the above inequality $(4q)^{l(x)-1} < p_1 \dots p_{l(x)-1}$ for large enough x . Our sequence $\{p_i\}_{i \geq 1}$, though not equal to the sequence of prime numbers $\{P_i\}_{i \geq 1}$, is obtained from the set P of all primes by removing a finite number of primes - those dividing m , hence when x goes to ∞ it behaves just as P does.*

AFTERTHOUGHTS 3. *A polynomial $f \in \mathbb{Z}[X]$ is called a Bouniakowsky Polynomial if f is irreducible, $\deg f > 1$ and $\gcd(f(1), f(2), \dots) = 1$.*

Theorem 1 (Bouniakowsky Conjecture). *A Bouniakowsky polynomial takes prime values for infinitely many values of x .*

If the Bouniakowsky Conjecture is true, then we can easily prove that $d((n^2 + 1)^t)$, where t is a fixed positive integer, doesn't eventually become monotonic. Indeed, assume the contrary and suppose $d((n^2 + 1)^t)$ is monotonic from some point $n \geq n_0$. If the Conjecture is true, $n^2 + 1 > n_0$ is a prime for infinitely many values of n . For such values, $n^2 + 1 = p$, and $d((n^2 + 1)^t) = d(p^t) = t + 1$. This, together with the monotonicity of the sequence would imply that $d((n^2 + 1)^t) \leq t + 1, \forall n \geq n_0$. However we have proven before that $n^2 + 1$ can have an arbitrarily large number of divisors.

REFERENCES

- 1 S. L. Berlov, S. V. Ivanov, K. P. Kohasi, *St. Petersburg Mathematical Olympiads*