Problems in Elementary Number Theory

Article contributions are always welcome. **Problems in Elementary Number theory** is devoted to the publication of expository papers in elementary number theory. You have to choose one (or two) of the problems from **PEN Problems Book**. Manuscripts should be written in English. Please, submit your articles in (the compiled) **PDF** file to PEN Team at **pen@problem-solving.be**.

Author: 'Put your name.'
Email: 'Put your email address.'
Date: 'Put the submission date.'

Contents

Chapter 1

Your draft

1.1 Put the title, here.

1 State the PEN Problem what you choose from **PEN Problems Book**.

PEN #

First Solution. First Solution □

Second Solution. Second Solution □

Third Solution. Third Solution □

Fourth Solution. Fourth Solution □

References and Further Reading

1 Book X

2 Book Y

3 Book Z

Chapter 2

Two Sample Articles

2.1 On the monotonicity of the divisor function

2
PEN J11

(a) *Saint-Peterburg, 1998* Let $d(n)$ denote the number of positive divisors of the 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 $d < \dfrac{n^2+1}{d}$. Clearly d is odd and less than n. Hence we have at most $\dfrac{n}{2}$ 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 2.1.1. *It must be mentioned that the problem was proposed for the Elemination 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 2.1.1. *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 $\pmod p$, 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 $s_i \mid r_i^2+m^2$. 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 2.1.1. $\gcd(a^2+m^2,(a-1)^2+m^2)=1$ *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 $\gcd(2a-1,4m^2+1)=1$. □

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 $f_{x-1}f_x \le f_{x^2-x+m^2}$, 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 2.1.2. *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 $b_i \not| 2h(x)+1 = 8x^2-2\lambda+1$, $\forall i=\overline{1,s}$. Since b_i's are odd, the last condition is equivalent to $b_i \not| (4x)^2-(4\lambda-2)$. 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 $\dfrac{b_i-1}{2}$ 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 $\lambda = \dfrac{L-2}{4}$. Clearly we can assume $\lambda > 0$. □

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

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

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 $f(p_1 \ldots p_k)$. Let $(p_1 \ldots p_k)^2 + m^2 = \prod_{i=1}^{s} q_i^{\alpha_i}$. 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

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

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

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 $h(\alpha_1, \alpha_2, \ldots, \alpha_s) \leq h(\alpha_1 - 1, \alpha_2, \ldots, \alpha_s, 1)$. By repeated applications of this inequality until $\alpha_i = 1$, for all i, we obtain the following inequality

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

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 $p_1 \ldots p_v < x \leq p_1 \ldots p_{v+1}$. Using once again the monotonicity of f, we establish the following upper bound for the function f:

$$f(x) \leq f\left(p_1 \ldots p_{l(x)}\right) \leq T^{l(x)}$$

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

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

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 $(4q)^{l(x)-1} < p_1 \ldots p_{l(x)-1}$ holds for large enough x. By the definition of $l(x)$, we have then, indeed, $p_1 \ldots p_{l(x)-1} < x$, obtaining $l(x) - 1 < \log_{4q} x$, what we wanted.

□

AFTERTHOUGHTS 2.1.2 (About the sequence $\{p_i\}_{i \geq 1}$)**.** *We omitted proof of the validity of the above inequality $(4q)^{l(x)-1} < p_1 \ldots p_{l(x)-1}$ 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 2.1.3. *A polynomial $f \in \mathbb{Z}[X]$ is called a Bouniakowsky Polynomial if f is irreducible,* $\deg f > 1$ *and* $\gcd(f(1), f(2), \ldots)) = 1$.

Theorem 2.1.1 (Bouniakowsky Conjecture)**.** *A Bouniakowsky polynomial takes prime values for infinitely many valuos 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. Peterburg Mathematical Olympiads*

2.2 Different Approaches to an Intuitive Problem

3 PEN N17 Suppose that a and b are distinct real numbers such that:

$$a-b, a^2-b^2, \cdots, a^k-b^k, \cdots \tag{2.1}$$

are all integers. Show that a and b are integers.

First Solution. Let $x_n = a^n - b^n$. We are given that $x_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$. We can easily deduce that a, b are rational: $\frac{\frac{x_2}{x_1} \pm x_1}{2} = \frac{a+b\pm(a-b)}{2} = a, b$.
Assume, for contradiction's sake, that a is not an integer. We'll have $a = \frac{p}{q}, (p,q) = 1$, and $|q| > 1$. There exist $m \in \mathbb{N}_0$ such that $q^m \mid a-b, q^{m+1} \nmid a-b$. We have $\left(x_1 + \frac{p}{q}\right)^n - \left(\frac{p}{q}\right)^n = x_n$, or equivalently:

$$\left(x'q^{m+1} + p\right)^n - p^n = q^n x_n \tag{2.2}$$

For a suitable integer x'. Now we'll use the binomial theorem and divide by q^{m+1}:

$$\sum_{i=0}^{n-1} \binom{n}{i} p^i {x'}^{n-i} q^{(m+1)(n-i-1)} = q^{n-m-1} x_n. \tag{2.3}$$

Looking (mod q), for $n > m+1$, we see that: $x'p^{n-1}n \equiv 0 \pmod q$. Exploiting the fact that $(q,p) = 1$ and taking $n = (m+2)|q| + 1$, yields $q|x'$, a contradiction. Hence, $q = \pm 1$ and a is an integer. $b = a - x_1$ is thus also an integer, Q.E.D.

□

Remark: notice the similarities to the proof of the Rational root theorem.

Second Solution. Notice the following identity:

$$x_{n+1}^2 - x_n x_{n+2} = (ab)^n x_1^2 \tag{2.4}$$

It can be proved directly for every natural n:
$x_n x_{n+2} - x_{n+1}^2 = (a^n - b^n)\left(a^{n+2} - b^{n+2}\right) - \left(a^{n+1} - b^{n+1}\right)^2 = a^{2n+2} - b^2 (ab)^n - a^2 (ab)^n + b^{2n+2} - a^{2n+2} + 2(ab)^{n+1} - b^{2n+2} = (ab)^n (a-b)^2 = (ab)^n x_1^2$.
The motivation for it is the known identity $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$ satisfied by the Fibonacci sequence: $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$ for all $n \in \mathbb{N}_0$. x_n is a linear recurrence sequence, with its first term being 0 (if we consider x_0), like F_n. From its form we deduce that the roots of its characteristic equation are a and b. Thus, given that $a \neq b$, the equation is $x^2 - (a+b)x + ab = 0$, hence x_n follows that recursion $x_{n+2} = (a+b)x_{n+1} - abx_n$.

Assume to the contrary that ab is not an integer. It can be represented in the form $\frac{p}{q}$, where p, q are relatively prime integers and $|q| > 1$. From (2.22), we have: $q^n | x_1^2 p^n$ For all n (because the expression on the left is an integer). From the fact that $(p,q) = 1$ it follows that $q^n | x_1^2$. x_1 is non-zero, hence $x_1^2 \geq q^n \geq 2^n$. This is true for all $n \in \mathbb{N}$ and it's a contradiction. Hence $|q| = 1$

and ab is an integer. $a-b=x_1$ is an integer also. Let $a=\frac{p_1}{q}, b=\frac{p_2}{q}$ $(p_{1,2},q\in\mathbb{Z})$. We know that $q^2|p_1p_2, q|p_1-p_2$. We'll manipulate it as follows:

$$q^2 \mid (p_1-p_2)^2+4p_1p_2=(p_1+p_2)^2 \implies q \mid p_1 \pm p_2 \implies q \mid 2p_{1,2} \tag{2.5}$$

We have 2 options: either a and b are both integers, or are half-integers, i.e. take the form $k_{1,2}+0.5$ for some integers $k_{1,2}$. We can see that the 2nd option is not valid in two different ways:
1. $a^n-b^n\in\mathbb{Z}$ is equivalent to $2^n \mid (2k_1+1)^n-(2k_2+1)^n$. For $n=2^l$ We can factor it as follows:

$$(2k_1+1)^{2^l}-(2k_2+1)^{2^l}=2(k_1-k_2)\prod_{i=0}^{l-1}\left((2k_1+1)^{2^i}+(2k_2+1)^{2^i}\right) \tag{2.6}$$

An expression of the form $a^{2^i}+b^{2^i}$, where a,b are odd and i is positive, is never divisible by 4. This is a direct consequence of $t^2\equiv 1 \pmod 4$ for $t\equiv 1 \pmod 2$ (choose $t=a^{2^{i-1}}, b^{2^{i-1}}$). Hence:

$$ord_2\left((2k_1+1)^{2^l}-(2k_2+1)^{2^l}\right)=l+ord_2\left((k_1-k_2)\left((2k_1+1)^2+(2k_2+1)^2\right)\right) \tag{2.7}$$

For all $l\in\mathbb{N}$. This fact contradicts $ord_2\left((2k_1+1)^n-(2k_2+1)^n\right)\geq n$ for all $n\in\mathbb{N}$: just take $n=2^l$ large enough.
2. We get that $ab=k_1k_2+\frac{2k_1+2k_2+1}{4}$ is an integer, which is impossible (shorter, huh?). □

Third Solution. We'll prove 3 lemmas.
<u>Lemma 1:</u> For any odd prime p, and distinct a,b satisfying $a-b\equiv 0 \pmod p, (a,b,p)=1$, one has $ord_p(a^n-b^n)=ord_p(n)+ord_p(a-b)$.
<u>Proof:</u> it is equivalent to the identity

$$\left(a+bp^k\right)^{p^st}-a^{p^st}\equiv a^{p^st-1}btp^{s+k} \pmod{p^{s+k+1}} \tag{2.8}$$

for $k>0$. It can be proved either by induction on $s\geq 0$, or by direct expanding:

$$\left(a+bp^k\right)^{p^st}-a^{p^st}=a^{p^st-1}btp^{s+t}+\sum_{i=2}^{p^st}\binom{p^st}{i}a^{p^st-i}p^{ki}b^i \tag{2.9}$$

It is enough to show that $ord_p\left(p^{ki}\binom{p^st}{i}\right)\geq k+s$ for $i>1$. Notice the following identity:

$$i\binom{p^st}{i}=p^st\binom{p^st-1}{i-1} \tag{2.10}$$

which implies: $ord_p\left(p^{ki}\binom{p^st}{i}\right)\geq ki+s-ord_pi$.
If we put $i=p^jl>1, (p,l)=1$, we get: $ki+s-ord_pi=kp^jl+s-j\geq k3^jl+s-j$. What we want to show is: $k\left(3^jl-1\right)\geq j+1$. We have $k\geq 1$ as a condition.
For $j=0$: $k\left(3^jl-1\right)\geq 3^jl-1=l-1\geq 1=j+1$, because $i=l>1$.
If $j>0$: $k\left(3^jl-1\right)\geq 3^j-1\geq j+1$ (follows from $3^j\geq j+2$ for $j\in\mathbb{N}$ - straightforward induction).
The result follows.
<u>Lemma 2:</u> For any distinct odd integers a, b we have $ord_2(a^n-b^n)=ord_2\left(\frac{a^2-b^2}{2}\right)+ord_2(n)$ for even $n\in\mathbb{N}$, and $ord_2(a^n-b^n)=ord_2(a-b)$ for odd $n\in\mathbb{N}$.
<u>Proof:</u> Both results follow directly from our work in the previous solution, and from the congruence

$\frac{a^n-b^n}{a-b}=\sum_{i=0}^{n-1}a^ib^{n-i-1}\equiv n\equiv 1 \pmod 2$ for odd n.
Lemma 3: For any positive number x, any real number y, and any prime p, the inequality $ord_p(n)\geq xn+y$ holds only for finitely many $n's$.
Proof: First step - let l be a non-negative integer. There are finitely many values of n that satisfy the inequality when $p^l||n$, namely: $n\leq\frac{l-y}{x}$. Second step - $p^l\geq l^{1.5}$ (induction). Third and last step - there are finitely many values of l that satisfy the inequality when $p^l||n$: $ord_p(n)\geq xn+y\implies l\geq xl^{1.5}+y$, or: $1\geq x\sqrt{l}+\frac{y}{l}$. When l tends to infinity, the last expression tends to ∞, which yields the result.
Combining the 3 steps, we get the result stated by the lemma.
Now, as before, we let $a=\frac{x}{z},b=\frac{y}{z}$ $(x\neq y)$. x_n is an integer for all $n\in\mathbb{N}$ is equivalent to:

$$\forall n\in\mathbb{N},z^n\mid x^n-y^n \tag{2.11}$$

We'll prove that $z\mid(x,y)$, and it will solve the problem. Set $g=(x,y),x'=\frac{x}{g},y'=\frac{y}{g}$.

Let p be an odd prime dividing z and set $k=ord_p(z)$. $x-y$ is divisible by z and hence by p. Also, denote o_p as the order of $x'y'^{-1}$ in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ (in the case when $(x',p)=(y',p)=1$), i.e. the minimal number such that $p|x'^{o_p}-y'^{o_p}$.
If $o_p\nmid n$, or one of x',y' is divisible by p: because $ord_p(z)$ reduces multiplication to addition,

$$ord_p(x^n-y^n)=ord_p(x'^n-y'^n)+ord_p(g^n)=n\ ord_p(g) \tag{2.12}$$

If $o_p\mid n$: from the first lemma -

$$\begin{aligned}
&ord_p(x^n-y^n)\\
&\qquad= ord_p(x'^n-y'^n)+ord_p(g^n)\\
&\qquad= ord_p(x'^{o_p}-y'^{o_p})+ord_p\left(\frac{n}{o_p}\right)+n\ ord_p(g)\\
&\qquad= C+ord_p(n)+n\ ord_p(g)
\end{aligned}$$

Combining those, we get the inequality: $nk=ord_p(z^n)\leq ord_p(x^n-y^n)\leq n\ ord_p(g)+|C|+ord_p(n)$, where C is suitable constant. By the 3rd lemma, it is possible for all n only if $ord_p(g)\geq k$.
The treatment of $p=2$ is exactly the same using the 2nd lemma, except for the value of C, and we get $ord_2(x^n-y^n)\leq n\ ord_2(g)+ord_p(n)+|C|$ for a suitable constant C. By the 3rd lemma, it is possible only if $ord_2(g)\geq k$.
The result follows. □

Generalizations:

Proposition 2.2.1. *Suppose that a and b are distinct real numbers such that: $a^n-b^n\in\mathbb{Z}$ for any $n\in\mathbb{N}$ divisible by s or t, where s,t are relatively prime positive integers. Then a,b are integers.*

Proof. It follows from the original problem: apply our result, once with $a=a'^s,b=b'^s$ and once with $a=a'^t,b=b'^t$. We get that a^s,b^s,a^t,b^t are integers. In the case where both a and b are non-zero, by Bzout's lemma there are integers $k_{1,2}$ such that $sk_1+tk_2=1$. We get: $a=(a^s)^{k_1}(a^t)^{k_2}\implies a\in\mathbb{Q}$. Together with $a^s\in\mathbb{Z}$ we get that $a\in\mathbb{Z}$. In the same way, $b\in\mathbb{Z}$. If

$a = b = 0$, we're done. If exactly one of $a = 0$, $b = 0$ is true, WLOG $a = 0$, as before we conclude that $b^s, b^t \in \mathbb{Z}$, and then $b \in \mathbb{Z}$. $\square$

Proposition 2.2.2. *Suppose that a and b are distinct rational numbers such that: $a^n - b^n \in \mathbb{Z}$ for infinitely many $n \in \mathbb{N}$. Then a, b are integers.*

Proof. We could actually show this already in the third solution. We again reformulate the problem as follows - $z^n \mid x^n - y^n$ for infinitely many n's implies $z \mid (x, y)$ (when $x \neq y$). As before, we use the 3rd lemma and get $ord_p((x, y)) \geq ord_p z$, for all primes p dividing z, and the result follows. $\square$

References and Further Reading

1 *PEN Problem N17*, http://www.mathlinks.ro/viewtopic.php?t=150843

2 *A nice and tricky lemma (lifting the exponent) by Santiago Cuellar and Jose Alejandro Samper*, http://reflections.awesomemath.org/2007_3/Lifting_the_exponent.pdf