

0.1 Different Approaches to an Intuitive Problem

1 Suppose that a and b are distinct real numbers such that:

PEN N17

$$a - b, a^2 - b^2, \dots, a^k - b^k, \dots \quad (1)$$

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: $\frac{x_2 \pm x_1}{2} = \frac{a+b \pm (a-b)}{2} = a, b$.

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:

$$(x'q^{m+1} + p)^n - p^n = q^n x_n \quad (2)$$

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

$$\sum_{i=0}^{n-1} \binom{n}{i} p^i x'^{n-i} q^{(m+1)(n-i-1)} = q^{n-m-1} x_n. \quad (3)$$

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 $q \mid x'$, 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:

$$x_{n+1}^2 - x_n x_{n+2} = (ab)^n x_1^2 \quad (4)$$

It can be proved directly for every natural n :

$$x_n x_{n+2} - x_{n+1}^2 = (a^n - b^n)(a^{n+2} - b^{n+2}) - (a^{n+1} - b^{n+1})^2 = a^{2n+2} - b^2(ab)^n - a^2(ab)^n + b^{2n+2} - a^{2n+2} + 2(ab)^{n+1} - b^{2n+2} = (ab)^n(a-b)^2 = (ab)^n x_1^2.$$

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 $n \in \mathbb{N}_0$. From the form of x_n we deduce that the roots of its characteristic equation are a and b , hence x_n follows that recursion $x_{n+2} = (a+b)x_{n+1} - abx_n$. Both x_n and F_n are linear recurrence sequences, with the zero term being 0 ($x_0 = a^0 - b^0 = 0$). The first term is not necessarily the same and we find out that we should multiply by x_1^2 in (4).

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 (4), we have: $q^n \mid x_1^2 p^n$ For all n (because the expression on the left is an integer). From the fact that $(p, q) = 1$ it follows that $q^n \mid x_1^2$. 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 $q^2 | p_1 p_2, q | p_1 - p_2$. We'll manipulate it as follows:

$$q^2 | (p_1 - p_2)^2 + 4p_1 p_2 = (p_1 + p_2)^2 \implies q | p_1 \pm p_2 \implies q | 2p_{1,2} \quad (5)$$

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 $2^n | (2k_1 + 1)^n - (2k_2 + 1)^n$. For $n = 2^l$ we can factor it as follows:

$$(2k_1 + 1)^{2^l} - (2k_2 + 1)^{2^l} = 4(k_1 - k_2)(k_1 + k_2 + 1) \prod_{i=1}^{l-1} \left((2k_1 + 1)^{2^i} + (2k_2 + 1)^{2^i} \right) \quad (6)$$

If $k_1 + k_2 + 1 = 0$ we are done, because we'll have $2^n | (2k_1 + 1)^n - (2k_2 + 1)^n = 2(2k_1 + 1)^n$ for all odd n , a contradiction. Otherwise -

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:

$$\text{ord}_2 \left((2k_1 + 1)^{2^l} - (2k_2 + 1)^{2^l} \right) = l + 2 + \text{ord}_2 \left((k_1 - k_2)(k_1 + k_2 + 1) \right) \quad (7)$$

For all $l \in \mathbb{N}$. This fact contradicts $\text{ord}_2 \left((2k_1 + 1)^n - (2k_2 + 1)^n \right) \geq n$ for all $n \in \mathbb{N}$: just take $n = 2^l$ large enough.

2. We get that $ab = k_1 k_2 + \frac{2k_1 + 2k_2 + 1}{4}$ is an integer, which is impossible. \square

Third Solution. We'll prove 3 lemmas.

Lemma 1: For any odd prime p , and distinct a, b satisfying $a - b \equiv 0 \pmod{p}, (a, b, p) = 1$, one has $\text{ord}_p(a^n - b^n) = \text{ord}_p(n) + \text{ord}_p(a - b)$.

Proof: it is equivalent to the identity

$$(a + bp^k)^{p^{s+t}} - a^{p^{s+t}} \equiv a^{p^{s+t-1}} b t p^{s+k} \pmod{p^{s+k+1}} \quad (8)$$

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

$$(a + bp^k)^{p^{s+t}} - a^{p^{s+t}} = a^{p^{s+t-1}} b t p^{s+k} + \sum_{i=2}^{p^{s+t}} \binom{p^{s+t}}{i} a^{p^{s+t-i}} p^{ki} b^i \quad (9)$$

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

$$i \binom{p^{s+t}}{i} = p^{s+t} \binom{p^{s+t}-1}{i-1} \quad (10)$$

which implies: $\text{ord}_p \left(p^{ki} \binom{p^{s+t}}{i} \right) \geq ki + s - \text{ord}_p i$.

If we put $i = p^j l > 1, (p, l) = 1$, we get: $ki + s - \text{ord}_p i = kp^j l + s - j \geq k3^j l + s - j$. What we want to show is: $k(3^j l - 1) \geq j + 1$. We have $k \geq 1$ as a condition.

For $j = 0$: $k(3^j l - 1) \geq 3^j l - 1 = l - 1 \geq 1 = j + 1$, because $i = l > 1$.

If $j > 0$: $k(3^j l - 1) \geq 3^j - 1 \geq j + 1$ (follows from $3^j \geq j + 2$ for $j \in \mathbb{N}$ - straightforward induction).

The result follows.

Lemma 2: For any distinct odd integers a, b we have $\text{ord}_2(a^n - b^n) = \text{ord}_2 \left(\frac{a^2 - b^2}{2} \right) + \text{ord}_2(n)$ for

even $n \in \mathbb{N}$ (when $a^2 \neq b^2$), and $\text{ord}_2(a^n - b^n) = \text{ord}_2(a - b)$ for odd $n \in \mathbb{N}$.

Proof: Both results follow directly from our work in the previous solution, and from the congruence $\frac{a^n - b^n}{a - b} = \sum_{i=0}^{n-1} a^i b^{n-i-1} \equiv n \equiv 1 \pmod{2}$ for odd n .

Lemma 3: For any positive number x , any real number y , and any prime p , the inequality $\text{ord}_p(n) \geq xn + y$ 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 $p^l | n$: $\text{ord}_p(n) \geq xn + y \implies l \geq x\sqrt{l} + \frac{y}{l}$. 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 $a = \frac{x}{z}, b = \frac{y}{z}$ ($x \neq y$). From now on we assume that $x^2 \neq y^2$ (this case is simpler). x_n is an integer for all $n \in \mathbb{N}$ is equivalent to:

$$\forall n \in \mathbb{N}, z^n \mid x^n - y^n \quad (11)$$

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 $k = \text{ord}_p(z)$. $x - y$ is divisible by z and hence by p . Also, denote o_p as the order of $x'y'^{-1}$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ (in the case when $(x', p) = (y', p) = 1$), i.e. the minimal number such that $p \mid x'^{o_p} - y'^{o_p}$.

If $o_p \nmid n$, or one of x', y' is divisible by p : because $\text{ord}_p(z)$ reduces multiplication to addition,

$$\text{ord}_p(x^n - y^n) = \text{ord}_p(x'^n - y'^n) + \text{ord}_p(g^n) = n \text{ord}_p(g) \quad (12)$$

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

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

Combining those, we get the inequality: $nk = \text{ord}_p(z^n) \leq \text{ord}_p(x^n - y^n) \leq n \text{ord}_p(g) + |C| + \text{ord}_p(n)$, where C is a suitable constant. By the 3rd lemma, it is possible for all n only if $\text{ord}_p(g) \geq k$.

The treatment of $p = 2$ is exactly the same using the 2nd lemma, except for the value of C , and we get $\text{ord}_2(x^n - y^n) \leq n \text{ord}_2(g) + \text{ord}_p(n) + |C|$ for a suitable constant C . By the 3rd lemma, it is possible only if $\text{ord}_2(g) \geq k$.

The result follows. □

Generalizations:

Proposition 0.1.1. *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, k_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 0.1.2. *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 $\text{ord}_p((x, y)) \geq \text{ord}_p z$, 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