Irrational numbers whose powers have a nice property

Pascual Restrepo Mesa

Abstract

The purpose of this article is to tackle a problem inspired by other problems of the same kind. The problem suggests the existence of irrational numbers with a nice property of their perfect powers: the residue of their power's integer part modulo m is constant and can equal any given constant.

Lately, many spectacular problems which marry algebra and number theory have become popular in math circles. These problems all have elementary proofs, but these proofs are hard to find and use both number theoretic and algebraic tools. Before stating and proving our main result, we will take a short journey through some of the problems which inspired its development.

Problem 1. Let m be a positive integer. Prove that there exists an irrational number x such that the integer part of x^n is always 1 modulo m for all positive integers n.

Unknown source

Problem 2. Calculate the integer part of $(3+2\sqrt{2})^{2005}$.

Problem Solving Through Problems

Problem 3. Let $a_1, a_2, \ldots, a_k$ and $b_1, b_2, \ldots, b_k$ be integers such that, given any k-tuple of irrational numbers $x_1, x_2, \ldots, x_k$ all bigger than 1, there exists positive integers $n_1, n_2, \ldots, n_k$ and $m_1, m_2, \ldots, m_k$ such that

$$a_1 \left\lfloor x_1^{n_1} \right\rfloor + a_2 \left\lfloor x_2^{n_2} \right\rfloor + \ldots + a_k \left\lfloor x_k^{n_k} \right\rfloor = b_1 \left\lfloor x_1^{m_1} \right\rfloor + b_2 \left\lfloor x_2^{m_2} \right\rfloor + \ldots + b_k \left\lfloor x_k^{m_k} \right\rfloor .$$

Prove that $a_i = b_i$ for $i = 1, 2, \ldots, k$.

Mathlinks Contest, Gabriel Dospinescu

Actually, these problems can be solved without our result, but as we will see, our result (and the methods used for its proof) will easily tackle all of them, offering alternative solutions to the proposers'. Now, our result:

Theorem. Let m be an integer and $0 \le t < m$ be another fixed integer. Then there exists an irrational α such that:

$$\left\lfloor \alpha^k \right\rfloor \equiv t \pmod{m},$$

for every positive integer k.

It is worth noting two things about the theorem before proving it.

Firstly, the result is clearly a generalization of problem 1–so what makes it more interesting? The reason is that it seems much simpler to have all the powers of a number equal to 1 in $\mathbb{Z}_m$ because it is the multiplicative identity. Actually, if we allow integer numbers instead of irrationals, then the case $t = 1$ would be trivial as all other cases have$m | t^2 - t$.

Secondly, the result offers a simple proof of problem 3 (try to solve it without the theorem to find out how hard it is!) and a generalization of the techniques used to solve problem 2.

We are now ready for the proof. We divide the proof into two steps: we begin by defining some convenient numbers in terms of the roots of a polynomial and then we compute the integer part of their powers.

First step: Defining our number in terms of the roots of a polynomial.

If n is even, consider the polynomial

$$x^n - M(n-1)^{n-2} \prod_{i=0}^{n-2} \left(x - \frac{i}{n-1} \right) + 1,$$

and if n is odd, consider the polynomial

$$x^n - M(n-1)^{n-2} \prod_{i=0}^{n-2} \left(x - \frac{i}{n-1} \right) - 1,$$

where M is a sufficiently large multiple of m (this definition will be refinedlater). For each n, let us call its respective polynomial P_n. We will show that when m is large enough, P_n satisfies the following properties.

1^{st} property:

$$P_n = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + (-1)^n,$$

where the a_k's are integers such that $m \mid a_k$ for $n - 1 \geq k \geq 1$.

This property is easily proved noticing that the coefficients of $\prod_{i=0}^{n-2} \left(x - \frac{i}{n-1} \right)$ have denominators that divide $(n-1)^l$ with $l \leq n-2$, so when they get multiplied by $M(n-1)^{n-2}$ they become integers divisible by m (recall that we chose $m \mid M$).

2^{nd} property: P_n has $n - 1$ real roots in the interval $(0, 1)$ and a root greater than 1, also $P_n(1) < 0$.

This is a very strong analytic property. Consider the polynomial $\prod_{i=0}^{n-2} \left(x - \frac{i}{n-1} \right)$ and let $|\epsilon|$ be the smallest norm of its local minima and maxima in $(0, 1]$, including its value at the endpoints as critical values, that is

$$|\epsilon| < \left| \prod_{i=0}^{n-2} \left(1 - \frac{i}{n-1} \right) \right|.$$

Thus it is enough to pick $M \geq \frac{2}{\epsilon}$.

The critical points of $\prod_{i=0}^{n-2}\left(x - \frac{i}{n-1}\right)$ in $[0, 1]$ alternate in sign. The reason is that there is a critical point between $\frac{i}{n-1}$ and $\frac{i+1}{n-1}$ for $i = 0, 1, \ldots, n-2$ and the polynomial alternates signs in these intervals since it has roots in $\frac{i}{n-1}$. Also since for each of these critical points z we have

$$|z^n + (-1)^n| < 2 < M \left|\prod_{i=0}^{n-2}\left(z - \frac{i}{n-1}\right)\right|,$$

the sign of P_n equals the sign of $\prod_{i=0}^{n-2}\left(z - \frac{i}{n-1}\right)$, also evaluating $P_n(0)$ and $P_n(1) < 0$, we find that P_n changes sign n times in the interval $[0, 1]$ and therefore has $n-1$ roots in that interval and another one greater than 1, as we wanted to prove.

Now, let $r_1 > r_2 > \ldots > r_n$ be the roots of P_n. We have that $r_1 > 1 > r_2 > \ldots > r_n > 0$. The idea is to calculate the integer part of r_1^{2pn} for some p big enough.

Second step: Calculating integer parts of our number

Let us calculate the integer part of r_1^{kn}. We start by defining the number $s_k = r_1^k + r_2^k + \ldots + r_n^k$ which, according to Newton's formulas, satisfies $s_0 = n$, and s_k is an integer for $k = 1, 2, \ldots, n-1$.

But much more can be said about the sequence $\{s_i\}_{i=1}^{\infty}$, by observing that

$$0 = r_i^k P_n(r_i) = r_i^{k+n} + a_{n-1}r_i^{k+n-1} ... + a_1 r_i^{k+1} + (-1)^n r_i^k$$

and summing for $i = 1, 2, \ldots, n$, we obtain

$$s_{k+n} + a_{n-1}s_{k+n-1} + a_{n-2}s_{k+n-2} + \ldots + a_1 s_{k+1} + (-1)^n s_k.$$

By straightforward strong induction we find that all the terms in the sequence are integers. Looking at the recurrence modulo m and recalling that $a_{n-1} \equiv a_{n-2} \equiv \ldots \equiv a_1 \equiv 0 \pmod{m}$, we get again by induction that

$$s_{2pn} \equiv n \pmod{m},$$

for every positive integer p.

We arrive at the end of the proof. First observe that for a large enough integer p, we have

$$s_{2phn} = \left\lfloor \left({r_1}^{2pn}\right)^h \right\rfloor + 1.$$

This happens because $1 > r_2 > r_3 > \ldots > r_n > 0$, and therefore, for p large enough $1 > r_2^{2phn} + r_3^{2phn} + \ldots + r_n^{2phn} > 0$. This implies that $s_{2phn} > \left({r_1}^{2pn}\right)^h > s_{2phn} - 1$. Since $s_{2phn} - 1$ is an integer, then it is the integer part of $\left({r_1}^{2pn}\right)^h$.

From this last remark, we get that for all sufficiently large p:

$$\left\lfloor \left({r_1}^{2pn}\right)^h \right\rfloor \equiv s_{2phn} - 1 \equiv n - 1 \pmod{m}.$$

Putting $n = t+1$ we find that $\alpha = r_1^{2pn}$ satisfies the required property, but we need it to be an irrational number. We prove there exists a p such that r_1^{2pn} is irrational.

Assume by way of contradiction that r_1^{2pn} is rational for all sufficiently large p. Then r_1^{2n} must be rational, but since r_1 is an algebraic integer, r_1^{2n} must therefore be an integer. This implies that the minimal polynomial over $\mathbb{Z}$ of r_1 divides $x^{2n} - c$ and P_n, where c is some integer. Let Q be the minimal integer polynomial of r_1 over the integers, then all the roots of Q are of the form $\sqrt[2n]{c} \cdot \zeta$ where ζ is a root of unity. It follows that if q is a prime divisor of c, then $q \mid Q(0)$, but this implies that q divides $P_n(0) = (-1)^n$, a contradiction, from where we get $c = 1$ and $r_1 = 1$ which we know cannot happen because $P_n(1) < 0$.

This concludes the proof. However there are many open questions: what about rationals with this property? what about non-algebraic solutions? What about tracendental numbers with this property?

Exercises:

1. Solve first three problems. (repeat the method for problem 1)

2. Let S be a set such that for any $\alpha \in \mathbb{R} - \mathbb{Q}$, there is a number $n \in \mathbb{Z}^+$ such that $\lfloor \alpha^n \rfloor \in S$. Prove that S contains numbers with arbitrarily large sum of digits.

Gabriel Dospinescu

The problems were taken from Titu Andreescu and Gabriel Dospinescu's upcoming book Problems from the Book *and www.mathlinks.ro*

Author: Pascual Restrepo Mesa, Universidad de los Andes, Colombia

Email: p.restrepo23@uniandes.edu.co