A Formal Proof That $n^5 - n$ Is Divisible by 30 for Every Integer n

Agentic NL→Lean 4 Pipeline

April 20, 2026

Abstract

We prove that for every integer n, the quantity $n^5 - n$ is divisible by 30. We formally verified this classical number-theoretic identity in *Lean 4* using the *Mathlib* library. The proof reduces the claim to a finite check in the ring $\mathbb{Z}/30\mathbb{Z}$, which the kernel discharges by decidable evaluation. The takeaway is that a single decidable computation in $\mathbb{Z}/30\mathbb{Z}$ settles the divisibility uniformly for all integers.

1 Introduction

The identity $30 \mid n^5 - n$ is a classical consequence of Fermat's little theorem applied to the primes 2, 3, and 5. It generalizes the familiar fact that $n^3 - n$ is divisible by 6 and foreshadows the pattern captured by Euler's theorem. The result is a staple of introductory number theory and a convenient test case for automated divisibility reasoning.

Theorem 1. *For every $n \in \mathbb{Z}$, $30 \mid n^5 - n$.*

2 Formal Statement

```
theorem n_pow_five_sub_n_dvd_thirty (n : Z) : (30 : Z) | n^5 -
    n
```

3 Natural Language Proof

Let $n \in \mathbb{Z}$. We show $30 \mid n^5 - n$ by reducing modulo 30.

Consider the map $\pi : \mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$ sending an integer to its residue class. Since π is a ring homomorphism, $\pi(n^5 - n) = \pi(n)^5 - \pi(n)$.

We claim $m^5 - m = 0$ for every $m \in \mathbb{Z}/30\mathbb{Z}$. Because $\mathbb{Z}/30\mathbb{Z}$ has only 30 elements, this identity reduces to a finite computation: evaluate $m^5 - m$ at each

of the 30 residues and verify that each result equals 0. A direct check confirms all thirty cases.

Alternatively, by the Chinese Remainder Theorem, $\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Fermat's little theorem gives $m^2 \equiv m \pmod 2$, $m^3 \equiv m \pmod 3$, and $m^5 \equiv m \pmod 5$. From $m^2 \equiv m \pmod 2$ we obtain $m^5 = m \cdot (m^2)^2 \equiv m \pmod 2$, and from $m^3 \equiv m \pmod 3$ we obtain $m^5 = m^2 \cdot m^3 \equiv m^2 \cdot m = m^3 \equiv m \pmod 3$. Therefore $m^5 \equiv m$ modulo each of 2, 3, and 5, hence modulo 30.

Applying this to $m = \pi(n)$ yields $\pi(n^5 - n) = 0$ in $\mathbb{Z}/30\mathbb{Z}$. The kernel of π is exactly $30\mathbb{Z}$, so $30 \mid n^5 - n$. □

4 Formal Lean 4 Proof

The proof uses `decide` to verify the finite identity on $\mathbb{Z}/30\mathbb{Z}$, `push_cast` to transport the equation along the canonical map $\mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$, and `ZMod.intCast_zmod_eq_zero_iff_dvd` to convert the modular vanishing into integer divisibility.

```
import Mathlib

theorem n_pow_five_sub_n_dvd_thirty (n : Z) : (30 : Z) | n^5 -
    n := by
  have h : forall m : ZMod 30, m^5 - m = 0 := by decide
  have h2 : ((n^5 - n : Z) : ZMod 30) = 0 := by
    push_cast
    exact h _
  exact_mod_cast (ZMod.intCast_zmod_eq_zero_iff_dvd (n^5 - n)
      30).mp h2
```

5 Conclusion

We established that $30 \mid n^5 - n$ for every integer n by a finite check in $\mathbb{Z}/30\mathbb{Z}$. The argument is machine-verified in Lean 4 against Mathlib, leaving no informal gaps.