Lifting the Exponent

Maya Kądziołka

October 13, 2025

Abstract

We formalize the *Lifting the Exponent Lemma*, which shows how to find the largest power of p dividing $a^n \pm b^n$, for a prime p and positive integers a and b. The proof follows [1].

Contents

theory *LTE*
  imports
    HOL−Number-Theory.Number-Theory
begin

1 Library additions

lemma *cong-sum-mono-neutral-right*:
  assumes *finite T*
  assumes $S \subseteq T$
  assumes *zeros*: $\forall i \in T - S.\ [g\ i = 0]\ (mod\ n)$
  shows $[sum\ g\ T = sum\ g\ S]\ (mod\ n)$
⟨*proof*⟩

lemma *power-odd-inj*:
  fixes $a\ b :: 'a::linordered\text{-}idom$
  assumes *odd k* **and** $a\hat{}k = b\hat{}k$
  shows $a = b$
⟨*proof*⟩

lemma *power-eq-abs*:
  fixes $a\ b :: 'a::linordered\text{-}idom$
  assumes $a\hat{}k = b\hat{}k$ **and** $k > 0$
  shows $|a| = |b|$

$\langle proof \rangle$

lemma *cong-scale*:
$k \neq 0 \Longrightarrow [a = b]\ (mod\ c) \longleftrightarrow [k{*}a = k{*}b]\ (mod\ k{*}c)$
$\langle proof \rangle$

lemma *odd-square-mod-4*:
fixes $x :: int$
assumes $odd\ x$
shows $[x\hat{}2 = 1]\ (mod\ 4)$
$\langle proof \rangle$

2 The $p > 2$ case

context
fixes $x\ y :: int$ **and** $p :: nat$
assumes $prime\ p$
assumes $p\ dvd\ x - y$
assumes $\neg p\ dvd\ x \quad \neg p\ dvd\ y$
begin

lemma *decompose-mod-p*:
$[(\sum i{<}n.\ y\hat{}(n - Suc\ i) * x\hat{}i) = n{*}x\hat{}(n{-}1)]\ (mod\ p)$
$\langle proof \rangle$

Lemma 1:

lemma *multiplicity-diff-pow-coprime*:
assumes $coprime\ p\ n$
shows $multiplicity\ p\ (x\hat{}n - y\hat{}n) = multiplicity\ p\ (x - y)$
$\langle proof \rangle$

The inductive step:

lemma *multiplicity-diff-self-pow*:
assumes $p > 2$ **and** $x \neq y$
shows $multiplicity\ p\ (x\hat{}p - y\hat{}p) = Suc\ (multiplicity\ p\ (x - y))$
$\langle proof \rangle$

Theorem 1:

theorem *multiplicity-diff-pow*:
assumes $p > 2$ **and** $x \neq y$ **and** $n > 0$
shows $multiplicity\ p\ (x\hat{}n - y\hat{}n) = multiplicity\ p\ (x - y) + multiplicity\ p\ n$
$\langle proof \rangle$

end

Theorem 2:

corollary *multiplicity-add-pow*:
fixes $x\ y :: int$ **and** $p\ n :: nat$

assumes *odd n*
and *prime p* **and** $p > 2$
and *p dvd x + y* **and** $\neg$ *p dvd x* $\neg$ *p dvd y*
and $x \neq -y$
shows *multiplicity p (x^n + y^n) = multiplicity p (x + y) + multiplicity p n*
⟨*proof*⟩

3 The $p = 2$ case

Theorem 3:

theorem *multiplicity-2-diff-pow-4div*:
fixes *x y :: int*
assumes *odd x* *odd y* **and** *4 dvd x − y* **and** $n > 0$ $x \neq y$
shows *multiplicity 2 (x^n − y^n) = multiplicity 2 (x − y) + multiplicity 2 n*
⟨*proof*⟩

Theorem 4:

theorem *multiplicity-2-diff-even-pow*:
fixes *x y :: int*
assumes *odd x* *odd y* **and** *even n* **and** $n > 0$ **and** $|x| \neq |y|$
shows *multiplicity 2 (x^n − y^n) = multiplicity 2 (x − y) + multiplicity 2 (x + y) + multiplicity 2 n − 1*
⟨*proof*⟩

end

References

[1] Hossein Parvardi. Lifting The Exponent Lemma (LTE), 2011. URL: https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/lifting-the-exponent.pdf.