

A Formalisation of Lehmer's Primality Criterion

By Simon Wimmer and Lars Noschinski

May 29, 2023

Abstract

In 1927, Lehmer presented criteria for primality, based on the converse of Fermat's little theorem [2]. This work formalizes the second criterion from Lehmer's paper, a necessary and sufficient condition for primality.

As a side product we formalize some properties of Euler's φ -function, the notion of the order of an element of a group, and the cyclicity of the multiplicative group of a finite field.

Contents

1	Introduction	1
2	Lehmer's Theorem	1

1 Introduction

Section ?? provides some technical lemmas about polynomials. Section ?? to ?? formalize some basic number-theoretic and algebraic properties: Euler's φ -function, the order of an element of a group and an upper bound of the number of roots of a polynomial. Section ?? combines these results to prove that the multiplicative group of a finite field is cyclic. Based on that, Section 2 formalizes an extended version of Lehmer's Theorem, which gives us necessary and sufficient conditions to decide whether a number is prime.

theory *Lehmer*

imports

Main

HOL-Number-Theory.Residues

begin

2 Lehmer's Theorem

In this section we prove Lehmer's Theorem [2] and its converse. These two theorems characterize a necessary and complete criterion for primality. This

criterion is the basis of the Lucas-Lehmer primality test and the primality certificates of Pratt [3].

lemma *mod-1-coprime-nat*:
coprime a b if $0 < n$ *[* $a^n = 1$ *]* *(mod b) for* $a b :: nat$
 ⟨proof⟩

This is a weak variant of Lehmer's theorem: All numbers less than $p - 1$ must be considered.

lemma *lehmers-weak-theorem*:
assumes $2 \leq p$
assumes *min-cong1*: $\bigwedge x. 0 < x \implies x < p - 1 \implies [a^x \neq 1] \pmod{p}$
assumes *cong1*: $[a^{p-1} = 1] \pmod{p}$
shows *prime p*
 ⟨proof⟩

lemma *prime-factors-elem*:
fixes $n :: nat$ **assumes** $1 < n$ **shows** $\exists p. p \in \text{prime-factors } n$
 ⟨proof⟩

lemma *cong-pow-1-nat*:
 $[a^x = 1] \pmod{b}$ **if** $[a = 1] \pmod{b}$ **for** $a b :: nat$
 ⟨proof⟩

lemma *cong-gcd-eq-1-nat*:
fixes $a b :: nat$
assumes $0 < m$ **and** *cong-props*: $[a^m = 1] \pmod{b}$ $[a^n = 1] \pmod{b}$
shows $[a^{\text{gcd } m n} = 1] \pmod{b}$
 ⟨proof⟩

lemma *One-leq-div*:
 $1 < b \text{ div } a$ **if** $a \text{ dvd } b$ $a < b$ **for** $a b :: nat$
 ⟨proof⟩

theorem *lehmers-theorem*:
assumes $2 \leq p$
assumes *pf-notcong1*: $\bigwedge x. x \in \text{prime-factors } (p - 1) \implies [a^{(p-1) \text{ div } x} \neq 1] \pmod{p}$
assumes *cong1*: $[a^{p-1} = 1] \pmod{p}$
shows *prime p*
 ⟨proof⟩

The converse of Lehmer's theorem is also true.

lemma *converse-lehmer-weak*:
assumes *prime-p*: *prime p*
shows $\exists a. [a^{p-1} = 1] \pmod{p} \wedge (\forall x. 0 < x \longrightarrow x \leq p - 2 \longrightarrow [a^x \neq 1] \pmod{p})$
 $\wedge a > 0 \wedge a < p$
 ⟨proof⟩

theorem *converse-lehmer*:
assumes *prime-p:prime(p)*
shows $\exists a . [a^{p-1} = 1] \pmod{p} \wedge$
 $(\forall q. q \in \text{prime-factors}(p-1) \longrightarrow [a^{(p-1) \text{ div } q} \neq 1] \pmod{p})$
 $\wedge a > 0 \wedge a < p$
 ⟨*proof*⟩

end

References

- [1] K. Conrad. Cyclicity of $(\mathbf{Z}/(p))^\times$. <http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/cyclicFp.pdf>.
- [2] D. H. Lehmer. Tests for primality by the converse of fermat's theorem. *Bull. Amer. Math. Soc.*, 33:327–340, 1927.
- [3] V. R. Pratt. Every prime has a succinct certificate. *SIAM Journal on Computing*, 4(3):214–220, 1975.