A Formalisation of Lehmer’s Primality Criterion

By Simon Wimmer and Lars Noschinski

August 16, 2018

Abstract

In 1927, Lehmer presented criterions 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 \( \phi \)-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 \( \phi \)-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:**

\[
\text{co}\text{prime } a \text{ } b \text{ if } 0 < n \Rightarrow [a^n = 1] \pmod{b} \text{ for } a, b :: \text{nat}
\]

(\text{proof})

This is a weak variant of Lehmer’s theorem: All numbers less then \( p - 1 \) must be considered.

**Lemma lehmers-weak-theorem:**

\[
\text{assumes } 2 \leq p
\]
\[
\text{assumes } \text{min-cong1: } \forall x. 0 < x \Rightarrow x < p - 1 \Rightarrow [a^x \neq 1] \pmod{p}
\]
\[
\text{assumes } \text{cong1: } [a^\cdot (p - 1) = 1] \pmod{p}
\]
\[
\text{shows } \text{prime } p
\]

(\text{proof})

**Lemma prime-factors-elem:**

\[
\text{fixes } n :: \text{nat } \text{assumes } 1 < n \text{ shows } \exists p. p \in \text{prime-factors } n
\]

(\text{proof})

**Lemma cong-pow-1-nat:**

\[
[a^x = 1] \pmod{b} \text{ if } [a = 1] \pmod{b} \text{ for } a, b :: \text{nat}
\]

(\text{proof})

**Lemma cong-gcd-eq-1-nat:**

\[
\text{fixes } a, b :: \text{nat}
\]
\[
\text{assumes } 0 < m \text{ and } \text{cong-props: } [a^m = 1] \pmod{b} \text{ } [a^n = 1] \pmod{b}
\]
\[
\text{shows } [a^\cdot \text{gcd } m, n = 1] \pmod{b}
\]

(\text{proof})

**Lemma One-leq-div:**

\[
1 < b \text{ div } a \text{ if } a \text{ }\text{dvd } b \text{ } a < b \text{ for } a, b :: \text{nat}
\]

(\text{proof})

**Theorem lehmers-theorem:**

\[
\text{assumes } 2 \leq p
\]
\[
\text{assumes } \text{pf-notcong1: } \forall x. x \in \text{prime-factors } (p - 1) \Rightarrow [a^\cdot ((p - 1) \text{ div } x) \neq 1] \pmod{p}
\]
\[
\text{assumes } \text{cong1: } [a^\cdot (p - 1) = 1] \pmod{p}
\]
\[
\text{shows } \text{prime } p
\]

(\text{proof})

The converse of Lehmer’s theorem is also true.

**Lemma converse-lehmer-weak:**

\[
\text{assumes } \text{prime-p: prime } p
\]
\[
\text{shows } \exists a. [a^\cdot (p - 1) = 1] \pmod{p} \land (\forall x. 0 < x \Rightarrow x \leq p - 2 \Rightarrow [a^x \neq 1] \pmod{p})
\]
\[
\land a > 0 \land a < p
\]

(\text{proof})
**Theorem** converse-lehmer:

**Assumes** prime-\(p\): prime\(p\)

**Shows** \(\exists a. [a^{(p-1)} = 1] \pmod{p} \land (\forall q. q \in \text{prime-factors} (p-1) \longrightarrow [a^{((p-1) \div q)} \neq 1] \pmod{p}) \land a > 0 \land a < p\)

\(\langle \text{proof} \rangle\)

end

**References**

