A Formalisation of Lehmer's Primality Criterion

By Simon Wimmer and Lars Noschinski

December 14, 2021

Abstract

In 1927, Lehmer presented criterions for primality, based on the converse of Fermat's litte 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

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 then $p - 1$ must be considered.

lemma *lehmers-weak-theorem*:
assumes *2 ≤ p*
assumes *min-cong1*: ⋀*x*. *0 < x* ⟹ *x < p − 1* ⟹ [*a ^ x ≠ 1*] (*mod p*)
assumes *cong1*: [*a ^ (p − 1) = 1*] (*mod p*)
shows *prime p*
⟨*proof*⟩

lemma *prime-factors-elem*:
fixes *n* :: *nat* **assumes** *1 < n* **shows** ∃*p*. *p* ∈ *prime-factors n*
⟨*proof*⟩

lemma *cong-pow-1-nat*:
[*a ^ x = 1*] (*mod b*) **if** [*a = 1*] (*mod 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*] (*mod b*) [*a ^ n = 1*] (*mod b*)
shows [*a ^ gcd m n = 1*] (*mod b*)
⟨*proof*⟩

lemma *One-leq-div*:
1 < b div a **if** *a dvd b a < b* **for** *a b* :: *nat*
⟨*proof*⟩

theorem *lehmers-theorem*:
assumes *2 ≤ p*
assumes *pf-notcong1*: ⋀*x*. *x* ∈ *prime-factors* (*p − 1*) ⟹ [*a ^ ((p − 1) div x) ≠ 1*] (*mod p*)
assumes *cong1*: [*a ^ (p − 1) = 1*] (*mod p*)
shows *prime p*
⟨*proof*⟩

The converse of Lehmer's theorem is also true.

lemma *converse-lehmer-weak*:
assumes *prime-p*: *prime p*
shows ∃ *a*. [*a^(p − 1) = 1*] (*mod p*) ∧ (∀ *x* . *0 < x* ⟶ *x ≤ p − 2* ⟶ [*a^x ≠ 1*] (*mod p*))
∧ *a > 0* ∧ *a < p*
⟨*proof*⟩

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