

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 $0 < n$ $[a^n = 1] \pmod{b}$ for $a b :: nat$
proof –
from *that coprime-1-left* **have** *coprime $(a^n) b$*
using *cong-imp-coprime cong-sym* **by** *blast*
with $\langle 0 < n \rangle$ **show** *?thesis*
by *simp*
qed

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 (*rule totient-imp-prime*)
from $\langle 2 \leq p \rangle$ *cong1* **have** *coprime a p*
by (*intro mod-1-coprime-nat[of p - 1]*) *auto*
then **have** $[a^{\text{totient } p} = 1] \pmod{p}$
by (*intro euler-theorem*) *auto*
then **have** $\text{totient } p \geq p - 1 \vee \text{totient } p = 0$
using *min-cong1[of totient p]* **by** *fastforce*
moreover **have** $\text{totient } p > 0$
using $\langle 2 \leq p \rangle$ **by** *simp*
moreover **from** $\langle p \geq 2 \rangle$ **have** $\text{totient } p < p$ **by** (*intro totient-less*) *auto*
ultimately **show** $\text{totient } p = p - 1$ **by** *presburger*
qed (*insert $\langle p \geq 2 \rangle$, auto*)

lemma *prime-factors-elem*:
fixes $n :: nat$ **assumes** $1 < n$ **shows** $\exists p. p \in \text{prime-factors } n$
using *assms* **by** (*cases prime n*) (*auto simp: prime-factors-dvd prime-factor-nat*)

lemma *cong-pow-1-nat*:
 $[a^x = 1] \pmod{b}$ **if** $[a = 1] \pmod{b}$ **for** $a b :: nat$
using *cong-pow [of a 1 b x]* **that** **by** *simp*

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 –
obtain $c d$ **where** $\text{gcd } m n = m * c + n * d$ **using** *bezout-nat[of m n]* $\langle 0 < m \rangle$
by *auto*
have *cong-m*: $[a^{m * c} = 1] \pmod{b}$ **and** *cong-n*: $[a^{n * d} = 1] \pmod{b}$
using *cong-props* **by** (*simp-all only: cong-pow-1-nat power-mult*)

have $[1 * a^{\wedge} \text{gcd } m \ n = a^{\wedge} (n * d) * a^{\wedge} \text{gcd } m \ n] \text{ (mod } b)$
by *(rule cong-scalar-right, rule cong-sym) (fact cong-n)*
also have $[a^{\wedge} (n * d) * a^{\wedge} \text{gcd } m \ n = a^{\wedge} (m * c)] \text{ (mod } b)$
using gcd by *(simp add: power-add)*
also have $[a^{\wedge} (m * c) = 1] \text{ (mod } b)$ **using** *cong-m* **by** *simp*
finally show $[a^{\wedge} \text{gcd } m \ n = 1] \text{ (mod } b)$ **by** *simp*
qed

lemma *One-leq-div:*

$1 < b \text{ div } a$ **if** $a \text{ dvd } b$ $a < b$ **for** $a \ b :: \text{nat}$
using *that* **by** *(metis dvd-div-mult-self mult.left-neutral mult-less-cancel2)*

theorem *lehmers-theorem:*

assumes $2 \leq p$
assumes *pf-notcong1*: $\bigwedge x. x \in \text{prime-factors } (p - 1) \implies [a^{\wedge} ((p - 1) \text{ div } x) \neq 1] \text{ (mod } p)$
assumes *cong1*: $[a^{\wedge} (p - 1) = 1] \text{ (mod } p)$
shows *prime p*
proof *cases*
assume $[a = 1] \text{ (mod } p)$ **with** $\langle 2 \leq p \rangle$ *pf-notcong1* **show** *?thesis*
by *(metis cong-pow-1-nat less-diff-conv linorder-neqE-nat linorder-not-less one-add-one prime-factors-elem two-is-prime-nat)*

next

assume *A-notcong-1*: $[a \neq 1] \text{ (mod } p)$
{ fix } x **assume** $0 < x \ x < p - 1$
have $[a^{\wedge} x \neq 1] \text{ (mod } p)$
proof
assume $[a^{\wedge} x = 1] \text{ (mod } p)$
then have *gcd-cong-1*: $[a^{\wedge} \text{gcd } x \ (p - 1) = 1] \text{ (mod } p)$
by *(rule cong-gcd-eq-1-nat[OF <0 < x> - cong1])*

have $\text{gcd } x \ (p - 1) = p - 1$

proof *(rule ccontr)*

assume $\neg ?thesis$
then have *gcd-p1*: $\text{gcd } x \ (p - 1) \text{ dvd } (p - 1) \ \text{gcd } x \ (p - 1) < p - 1$
using *gcd-le2-nat[of p - 1 x] <2 ≤ p>* **by** *(simp, linarith)*

define *c* **where** $c = (p - 1) \text{ div } (\text{gcd } x \ (p - 1))$

then have *p-1-eq*: $p - 1 = \text{gcd } x \ (p - 1) * c$ **unfolding** *c-def* **using** *gcd-p1*
by *(metis dvd-mult-div-cancel)*

from *gcd-p1* **have** $1 < c$ **unfolding** *c-def* **by** *(rule One-leq-div)*

then obtain *q* **where** *q-pf*: $q \in \text{prime-factors } c$

using *prime-factors-elem* **by** *auto*

then have $q \text{ dvd } c$ **by** *auto*

have $q \in \text{prime-factors } (p - 1)$ **using** *q-pf <1 < c> <2 ≤ p>*

by *(subst p-1-eq) (simp add: prime-factors-product)*

moreover

```

    have [a ^ ((p - 1) div q) = 1] (mod p)
      by (subst p-1-eq,subst dvd-div-mult-self[OF ‹q dvd c›,symmetric])
        (simp del: One-nat-def add: power-mult gcd-cong-1 cong-pow-1-nat)
    ultimately
    show False using pf-notcong1 by metis
  qed
  then show False using ‹x < p - 1›
    by (metis ‹0 < x› gcd-le1-nat gr-implies-not0 linorder-not-less)
  qed
}
with lehmers-weak-theorem[OF ‹2 ≤ p› - cong1] show ?thesis by metis
qed

```

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 –

have $p \geq 2$ **by** (rule prime-ge-2-nat[OF prime-p])

obtain a **where** $a : a \in \{1 .. p - 1\} \wedge \{1 .. p - 1\} = \{a^i \pmod p \mid i . i \in UNIV\}$

using residue-prime-mult-group-has-gen[OF prime-p] **by** blast

{

{ **fix** x::nat **assume** $x : 0 < x \wedge x \leq p - 2 \wedge [a^x = 1] \pmod p$

have $\{a^i \pmod p \mid i . i \in UNIV\} = \{a^i \pmod p \mid i . 0 < i \wedge i \leq x\}$

proof

show $\{a^i \pmod p \mid i . 0 < i \wedge i \leq x\} \subseteq \{a^i \pmod p \mid i . i \in UNIV\}$ **by**

blast

{ **fix** y **assume** $y : y \in \{a^i \pmod p \mid i . i \in UNIV\}$

then obtain i **where** $i : y = a^i \pmod p$ **by** auto

define q r **where** $q = i \text{ div } x$ **and** $r = i \pmod x$

have $i = q * x + r$ **by** (simp add: r-def q-def)

hence $y = q * x + r = ((a^{q * x}) \pmod p) * ((a^r) \pmod p) \pmod p$

by (simp add: i power-add mod-mult-eq)

have $a^{q * x} \pmod p = (a^x \pmod p)^q \pmod p$

by (simp add: power-mod mult commute power-mult[symmetric])

then have $y = a^r \pmod p$ **using** ‹p ≥ 2› x

by (simp add: cong-def y-q-r)

have $y \in \{a^i \pmod p \mid i . 0 < i \wedge i \leq x\}$

proof (cases)

assume $r = 0$

then have $y = a^x \pmod p$ **using** ‹p ≥ 2› x

by (simp add: cong-def y-r)

thus ?thesis **using** x **by** blast

next

assume $r \neq 0$

thus ?thesis **using** x **by** (auto simp add: y-r r-def)

```

    qed
  }
  thus { $a^i \bmod p \mid i. i \in UNIV$ }  $\subseteq$  { $a^i \bmod p \mid i. 0 < i \wedge i \leq x$ } by auto
  qed
  note  $X = this$ 

  have  $p - 1 = \text{card } \{1 .. p - 1\}$  by auto
  also have  $\{1 .. p - 1\} = \{a^i \bmod p \mid i. 1 \leq i \wedge i \leq x\}$  using X a by auto
  also have  $\dots = (\lambda i. a^i \bmod p) \text{ ` } \{1..x\}$  by auto
  also have  $\text{card } \dots \leq p - 2$ 
    using Finite-Set.card-image-le[of  $\{1..x\} \lambda i. a^i \bmod p$ ]  $x$  by auto
  finally have False using  $\langle 2 \leq p \rangle$  by arith
}
}
hence  $\forall x. 0 < x \longrightarrow x \leq p - 2 \longrightarrow [a^x \neq 1] \pmod p$  by auto
} note a-is-gen = this
{
  assume  $a > 1$ 
  have  $\neg p \text{ dvd } a$ 
  proof (rule ccontr)
    assume  $\neg \neg p \text{ dvd } a$ 
    hence  $p \text{ dvd } a$  by auto
    have  $p \leq a$  using dvd-nat-bounds[OF -  $\langle p \text{ dvd } a \rangle$ ]  $a$  by simp
    thus False using  $\langle a > 1 \rangle$   $a$  by force
  qed
  hence coprime  $a p$ 
    using prime-imp-coprime-nat [OF prime-p] by (simp add: ac-simps)
  then have  $[a^{\text{totient } p} = 1] \pmod p$ 
    by (rule euler-theorem)
  also from prime-p have totient  $p = p - 1$ 
    by (rule totient-prime)
  finally have  $[a^{p-1} = 1] \pmod p$  .
}
}
hence  $[a^{p-1} = 1] \pmod p$  using  $a$  by fastforce
thus ?thesis using a-is-gen  $a$  by auto
qed

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 -
  have  $p \geq 2$  by (rule prime-ge-2-nat[OF prime-p])
  obtain  $a$  where  $a: [a^{p-1} = 1] \pmod p \wedge (\forall x. 0 < x \longrightarrow x \leq p - 2 \longrightarrow$ 
   $[a^x \neq 1] \pmod p)$ 
     $\wedge a > 0 \wedge a < p$ 
  using converse-lehmer-weak[OF prime-p] by blast
  { fix  $q$  assume  $q: q \in \text{prime-factors } (p - 1)$ 
    hence  $0 < q \wedge q \leq p - 1$  using  $\langle p \geq 2 \rangle$ 

```

```

    by (auto simp add: dvd-nat-bounds prime-factors-gt-0-nat)
  hence  $(p - 1) \operatorname{div} q \geq 1$  using div-le-mono[of  $q$   $p - 1$   $q$ ] div-self[of  $q$ ] by simp
  have  $q \geq 2$  using  $q$  by (auto intro: prime-ge-2-nat)
  hence  $(p - 1) \operatorname{div} q < p - 1$  using  $\langle p \geq 2 \rangle$  by simp
  hence  $[a^{(p - 1) \operatorname{div} q} \neq 1] \pmod{p}$  using a  $\langle (p - 1) \operatorname{div} q \geq 1 \rangle$ 
    by (auto simp add: Suc-diff-Suc less-eq-Suc-le)
}
thus ?thesis using a by auto
qed

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.