



HAL
open science

Primality Tests and Prime Certificate

Laurent Théry

► **To cite this version:**

| Laurent Théry. Primality Tests and Prime Certificate. 2022. hal-03601611

HAL Id: hal-03601611

<https://inria.hal.science/hal-03601611>

Preprint submitted on 8 Mar 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Primality Tests and Prime Certificate

Laurent Théry

Marelle Project - INRIA Sophia Antipolis

Abstract

This note presents a formalisation done in COQ of Lucas-Lehmer test and Pocklington certificate for prime numbers. They both are direct consequences of Fermat little theorem. Fermat little theorem is proved using elementary group theory and in particular Lagrange theorem.

1 Definitions and Notations

In order to present our formalisation, we first need to introduce some functions and predicates over natural numbers, lists and sets.

1.1 Natural numbers

The predicates over the natural numbers are the following:

- **Divisibility:** n divides m , written $n \mid m$, if there exists a number q such that $m = nq$.
- **Primality:** p is prime, written $prime(p)$, if p has *exactly* two positive divisors 1 and p .
- **CoPrimality:** p and q are co-prime, written $coprime(p, q)$, if 1 is their unique positive common divisor.
- **Modulo:** p is equal to q modulo n , written $p \equiv q [n]$, if n divides $p - q$.

and the functions are:

- **Gcd:** the greatest common divisor of two numbers p and q is written $p \wedge q$.
- **Quotient:** the integer quotient of the division of p by q is written p/q .
- **Remainder:** the remainder of the division of p by q is written $p \bmod q$.
- **Euler function:** $\Phi(n) = \sum_{i=1}^{n-1} (\text{if } \text{coprime}(i, n) \text{ then } 1 \text{ else } 0)$.

1.2 Lists

Lists are denoted as $[a_1, a_2, \dots, a_n]$. We write the size of a list L as $|L|$, the concatenation of two lists L_1, L_2 as $L_1 + L_2$ and the fact that an element a belongs to a list L as $a \in L$.

1.3 Sets

Sets are denoted as $\{a_1, a_2, \dots, a_n\}$. We write the size of a set G as $|G|$, the fact that an element a belongs to a set G as $a \in G$, the fact that a set G_1 is included in a set G_2 as $G_1 \subset G_2$. Over sets, we define the notions of finite monoid and finite group:

- **Finite Monoid:** $(G, *)$ is a finite monoid, iff

G is finite: $G = \{e, a_1, a_2, \dots, a_n\}$,

the operation $*$ is internal: if $a \in G$ and $b \in G$ then $ab \in G$,

the operation $*$ is associative: $a(bc) = (ab)c$,

the element e is neutral: $ea = a = ae$.

- **Finite Group:** $(G, *)$ is a finite group, iff

G is finite: $G = \{e, a_1, a_2, \dots, a_n\}$,

the operation $*$ is internal: if $a \in G$ and $b \in G$ then $ab \in G$,

the operation $*$ is associative: $a(bc) = (ab)c$,

the element e is neutral: $ea = a = ae$,

every element has an inverse: $aa^{-1} = e = a^{-1}a$.

A group $(H, *)$ is a subgroup of a group $(G, *)$ if $G \subset H$.

2 Basic Theorems

Four basic theorems are mainly needed for our development: Gauss theorem for division, Bezout theorem for gcd, the fact that $\Phi(p) = p - 1$ for p prime and Lagrange for the cardinality of subgroup.

Theorem 2.1 (Gauss) *If $m \mid np$ and $\text{coprime}(m, n)$ then $m \mid p$.*

This theorem does not belong to our development, nevertheless we outline its proof. The key point of the proof is that divisibility is compatible with the subtraction: if $m \mid n$ and $m \mid p$ then $m \mid n - p$. Now, we have the hypothesis $m \mid np$ and we also have that $m \mid mp$. Remembering Euclid algorithm and using the compatibility of the subtraction we can derive that $m \mid (m \wedge n)p$. As we have $\text{coprime}(m, n)$, we get the expected result $m \mid p$.

Theorem 2.2 (Bezout) *Let m and n be two integers, then there exist u and v such that $mu + nv = m \wedge n$.*

Once again the proof of this theorem follows Euclid algorithm to compute the gcd of m and n .

Theorem 2.3 *Let p be a prime number, $\Phi(p) = p - 1$*

Since p is prime, if $1 \leq i < p$ then $\text{coprime}(i, p)$, so $\Phi(p) = p - 1$.

Theorem 2.4 (Lagrange) *If $(H, *)$ is a subgroup of $(G, *)$ then $|H| \mid |G|$.*

Let $H = \{e, a_1, a_2, \dots, a_n\}$ and $G = \{e, b_1, b_2, \dots, b_m\}$, we have $H \subset G$. We build the increasing sequence $(L_i)_{i \leq m}$ of lists as follows:

$$L_0 = [e, a_1, a_2 \dots a_n];$$

$$\text{if } b_{i+1} \in L_i, L_{i+1} = L_i;$$

$$\text{if } b_{i+1} \notin L_i, L_{i+1} = [b_{i+1}e, b_{i+1}a_1, b_{i+1}a_2, \dots, b_{i+1}a_n] + L_i.$$

We use the convention that $a_0 = e$ and $b_0 = e$. It is easy to show that for all $i \leq m$ we have $|H| \mid |L_i|$ and $b_i \in L_m$. We are left with proving that $|L_m| = |H_m|$. To do so, we just need to show that the elements of H occurs only once in L_m . By contradiction, suppose b_k occurs more than once in L_m . There are two possibilities: either there exists i such that b_k occurs more than

once in L_i but not in L_{i-1} ¹, or b_k occurs in L_i and $L_i - L_{i-1}$. In the first case, there exist u and v , $b_i a_u = b_k = b_i a_v$. Simplifying by b_i^{-1} , we get $a_u = a_v$. So as G is a set, we have $u = v$. This contradicts the fact that b_k occurs more than once in L_i . In the second case, there exist u, v and j with $j < i$ such that $b_i a_u = b_k = b_j a_v$. Simplifying by a_u^{-1} , we get $b_i = b_j (a_v a_u^{-1})$. As $a_v \in G$ and $a_u \in G$, there exists a l such that $b_i = b_j a_l$, so $b_i \in L_j$. This contradicts the fact that $b_i \notin L_{i-1}$ that is true by construction since $L_i \neq L_{i-1}$.

3 Group of invertible elements

From a monoid we can extract a group by taking its invertible elements. This section explicits how this group is constructed and states some basic properties.

Definition 3.1 *Let $(G, *)$ be a finite monoid, we define $I(G)$ as $\{a \in G \mid \exists c \in G, ca = e = ac\}$.*

Theorem 3.1 *Let $(G, *)$ be a finite monoid, $(I(G), *)$ is a finite subgroup.*

$I(G)$ is finite since $I(G) \subset G$. The operation is internal since if a and b are in $I(G)$, then there exist c and d such that $ac = e = ca$ and $bd = e = db$. It follows that $(ab)(dc) = e = (dc)(ab)$ so $ab \in I(G)$. The operative is associative since $(G, *)$ is a monoid. We have $ee = e = ee$, so $e \in I(G)$ and as it is a neutral element in G , it is also a neutral element in $I(G)$. Every element has an inverse by construction.

Definition 3.2 *Given n , we define $\mathbb{Z}/n\mathbb{Z}$ as $\{i \mid 0 \leq i < n\}$.*

Definition 3.3 *Given n , we define the operation \otimes as $a \otimes b = (ab) \bmod n$.*

Theorem 3.2 *Given n , $(\mathbb{Z}/n\mathbb{Z}, \otimes)$ is a finite monoid.*

$\mathbb{Z}/n\mathbb{Z}$ is finite. The operation \otimes is internal since $0 \leq a \bmod n < n$. The operation is associative since $a \otimes (b \otimes c) = (abc) \bmod n = (a \otimes b) \otimes c$. 1 is a neutral element. Note that operation \otimes is also commutative.

Definition 3.4 *Given n , we define $(\mathbb{Z}/n\mathbb{Z})^*$ as $I(\mathbb{Z}/n\mathbb{Z})$.*

¹This includes also the degenerated case where b_k occurs twice in L_0

Theorem 3.3 Given n , $((\mathbb{Z}/n\mathbb{Z})^*, \otimes)$ is a finite group.

This is a direct consequence of Theorems 3.2 and 3.1.

Theorem 3.4 Given a number n , $|(\mathbb{Z}/n\mathbb{Z})^*| = \Phi(n)$.

Let $a \in (\mathbb{Z}/n\mathbb{Z})^*$, so there exists c such that $a \otimes c = 1$. So $(ac) \bmod n = 1$, $n \mid ac - 1$ and there exists a d such that $ac - dn = 1$ so by Theorem 2.2, we have $\text{coprime}(a, n)$. Reciprocally if $\text{coprime}(a, n)$ by Theorem 2.2 there exist u and v such that $ua + vn = 1$, so $u \otimes a = 1$.

Theorem 3.5 Given a prime number p , $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$.

This is a direct consequence of Theorems 2.3 and 3.4.

4 Order of an element

Given an element a of a group, we can construct a subgroup by repetitively multiplying a by itself. The cardinality of this subgroup is called the *order* of the element. This section explicits this constructed and state some basic properties. The last one is the famous Fermat Little Theorem which is at the base of Pocklington certificate.

Definition 4.1 Let $(G, *)$ be a finite group and a an element of G , we define $H_a = \{a^i \mid i \in \mathbb{N}\}$,

Note that in the definition, we take as convention that $a^0 = e$.

Definition 4.2 Let $(G, *)$ be a finite group and a be an element of G , we define $o(a)$, the order of the element a , as the smallest number such that there exists $k < o(a)$ such that $a^k = a^{o(a)}$.

First of all, H_a is finite since $H_a \subset G$. It follows there is a least one repetition in $[1, a, a^2, \dots, a^{|G|}]$. So the definition of $o(a)$ makes sense.

Theorem 4.1 Let $(G, *)$ be a finite group and a be an element of G , we have $a^{o(a)} = e$.

There exists $k < o(a)$ such that $a^k = a^{o(a)}$. Multiplying on both side by a^{-k} we get $a^0 = a^{o(a)-k}$. Since $o(a)$ was the smallest number for which there is a repetition, it implies that $k = 0$ and $a^{o(a)} = e$.

Theorem 4.2 *Let $(G, *)$ be a finite group, a be an element of G and n be a number, $a^n = e$ if and only if $o(a) \mid n$.*

Suppose $a^n = e$, by Definition 4.2, we have $o(a) \leq n$. Iteratively multiplying by $a^{-o(a)}$ on both side of the equation $a^n = e$ we get $a^{n \bmod o(a)} = e$. Since $n \bmod o(a) < o(a)$, it implies that $n \bmod o(a) = 0$ so $o(a) \mid n$. Conversely, suppose $o(a) \mid n$, so there exists k such that $n = ko(a)$. We have $a^n = a^{ko(a)} = (a^{o(a)})^k = e^k = e$.

Theorem 4.3 *Let $(G, *)$ be a finite group and a be an element of G , $H_a = \{1, a, a^2, \dots, a^{o(a)-1}\}$ and $|H_a| = o(a)$.*

This is a direct consequence of Definition 4.1 and Theorem 4.1.

Theorem 4.4 *Let $(G, *)$ be a finite group and a an element of G , $(H_a, *)$ is a finite subgroup of $(G, *)$.*

H_a is finite. The operation $*$ is internal since $a^i a^j = a^{i+j}$. The operation $*$ is associative since $a^i (a^j a^k) = a^{i+j+k} = (a^i a^j) a^k$. Every element has an inverse $a^i a^{o(a)-i} = e = a^{o(a)-i} a^i$. Note that this group is also commutative.

Theorem 4.5 *Let $(G, *)$ be a finite group and a an element of G , we have $o(a) \mid |G|$.*

This is a direct consequence of Theorem 2.4 and $|H_a| = o(a)$.

Theorem 4.6 *Let n be a number and $a \in (\mathbb{Z}/n\mathbb{Z})^*$, we have $o(a) \mid \Phi(n)$.*

This is a direct consequence of Theorems 4.5 and 3.4.

Theorem 4.7 *Let p be a prime number and $a \in (\mathbb{Z}/p\mathbb{Z})^*$, we have $o(a) \mid p-1$.*

This is a direct consequence of Theorems 4.5 and 3.5

Theorem 4.8 *Let n be a number and coprime(a, n) then $a^{\Phi(n)} \equiv 1 [n]$.*

As $a \wedge b = (a \bmod b) \wedge b$ and $a^i \equiv (a \bmod n)^i [n]$, we can restrict ourselves to the case in which $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Using Theorem 4.6, we have $o(a) \mid \Phi(n)$. By definition of the order, it follows that $a^{\Phi(n)} \equiv a^{ko(a)} \equiv (a^{o(a)})^k \equiv 1^k \equiv 1 [n]$ for some k .

Theorem 4.9 (Fermat Little Theorem) *If prime(p) and coprime(a, p) then $a^{p-1} \equiv 1 [p]$.*

This is a direct consequence of Theorems 2.3 and 4.8.

5 Lucas-Lehmer test

The previous sections have introduced all the material needed to present Lucas-Lehmer test. This test gives a direct way of checking primality for Mersenne numbers.

Definition 5.1 Let n be a number, we define K_n as $(\mathbb{Z}/n\mathbb{Z})^2$, i.e. $K_n = \{(a, b) \mid 0 \leq a \leq n \text{ and } 0 \leq b \leq n\}$.

Definition 5.2 we define the operation \oplus as $(a_1, b_1) \oplus (a_2, b_2) = ((a_1 + b_1) \bmod n, (b_1 + b_2) \bmod n)$.

Definition 5.3 we define the operation \odot as $(a_1, b_1) \odot (a_2, b_2) = ((a_1 a_2 + 3b_1 b_2) \bmod n, (a_1 b_2 + a_2 b_1) \bmod n)$.

Definition 5.4 we define the power as $(a, b)^n = \underbrace{(a, b) \odot (a, b) \dots (a, b)}_n$.

Definition 5.5 For $n > 1$, we define two elements of K_n w as $(2, 1)$, v as $(2, n - 1)$ and we define the sequence $(S_m)_{m \in \mathbb{N}}$ over the natural numbers such that $S_0 = 4$ and $S_{m+1} = S_m^2 - 2$.

Theorem 5.1 For $n > 1$, we have $w \odot v = (1, 0)$,

We have

$$\begin{aligned} w \odot v &= (2, 1) \odot (2, n - 1) \\ &= ((4 + 3(n - 1)) \bmod n, (2 * (n - 1) + 2) \bmod n) \\ &= (1, 0) \end{aligned}$$

Theorem 5.2 For $n > 1$, we have $w^{2^{m-1}} \oplus v^{2^{m-1}} = (S_m \bmod n, 0)$, for $m > 1$.

We prove this by induction.

If $m = 1$, we have $w + v = (2, 1) \oplus (2, n - 1) = (4 \bmod n, n \bmod n) = (4 \bmod n, 0)$.

If we suppose that $w^{2^{m-1}} \oplus v^{2^{m-1}} = (S_m \bmod n, 0)$, squaring on both side gives

$$(w^{2^{m-1}} \oplus v^{2^{m-1}}) \odot (w^{2^{m-1}} \oplus v^{2^{m-1}}) = (S_m \bmod n, 0) \odot (S_m \bmod n, 0)$$

Using the distributivity, commutativity and associativity gives us

$$(w^{2^m} \oplus v^{2^m}) \oplus (2, 0) \odot (w^{2^{m-1}} v^{2^{m-1}}) = (S_m^2 \bmod n, 0)$$

For the left side, using some properties of exponentiation we get:

$$\begin{aligned} (w^{2^m} \oplus v^{2^m}) \oplus (2, 0) \odot (w^{2^{m-1}} v^{2^{m-1}}) &= (w^{2^m} \oplus v^{2^m}) \oplus (2, 0) \odot ((wv)^{2^{m-1}}) \\ &= (w^{2^m} \oplus v^{2^m}) \oplus (2, 0) \odot (1, 0)^{2^{m-1}} \\ &= (w^{2^m} \oplus v^{2^m}) \oplus (2, 0) \end{aligned}$$

For the right side, using Definition 5.5 we get:

$$(S_m^2 \bmod n, 0) = ((S_{m+1} + 2) \bmod n, 0) = (S_{m+1} \bmod n, 0) \oplus (2, 0)$$

Simplifying by $(2, 0)$ on both side, we get

$$(w^{2^m} \oplus v^{2^m}) = (S_{m+1} \bmod n, 0)$$

Theorem 5.3 For $n > 1$ and $m > 1$, if we have $w^{2^{m-2}} \oplus v^{2^{m-2}} = (0, 0)$, then $w^{2^{m-1}} \neq (1, 0)$ and $w^{2^m} = (1, 0)$.

Multiplying the left side by $w^{2^{m-2}}$ we get

$$\begin{aligned} w^{2^{m-2}} \odot (w^{2^{m-2}} \oplus v^{2^{m-2}}) &= (w^{2^{m-2}} \odot w^{2^{m-2}}) \oplus (w^{2^{m-2}} \odot v^{2^{m-2}}) \\ &= w^{2^{m-1}} \oplus (wv)^{2^{m-2}} \\ &= w^{2^{m-1}} \oplus (1, 0)^{2^{m-2}} \\ &= w^{2^{m-1}} \oplus (1, 0) \end{aligned}$$

So we get $w^{2^{m-1}} = -(1, 0) = (n-1, 0) \neq (1, 0)$ since $n > 1$. Squaring $w^{2^{m-1}} = -(1, 0)$ we get $w^{2^m} = (1, 0)$.

Definition 5.6 (Mersenne numbers) M_p is the p th Mersenne if $M_p = 2^p - 1$.

Theorem 5.4 (Lucas-Lehmer Test) If $p > 2$ and $M_p \mid S_{p-1}$ then M_p is prime.

The proof is by contradiction. We suppose that M_p is composite, so there exists an n such that $1 < n \leq \sqrt{M_p}$ and $n \mid M_p$. We consider $K_n^* = I(K_n)$. As $(0, 0) \notin K_n^*$, we have $|K_n^*| \leq n^2 - 1 < M_p$. By Theorem 5.1, we have $w \odot v = (1, 0)$, so $w \in K_n^*$. We have $n \mid M_p$ and $M_p \mid S_{p-1}$, so $S_{p-1} \bmod n = 0$. By Theorem 5.2, we get $w^{2^{m-2}} \oplus v^{2^{m-2}} = (0, 0)$. By Theorem 5.3, we deduce that $w^{2^{m-1}} \neq (1, 0)$ and $w^{2^m} = (1, 0)$. By Theorem 4.2, we have $o(w) \mid 2^m$. We deduce that $o(w) = 2^p$ for some $p \leq m$. If $p < m$, we would have $w^{2^{m-1}} = w^{2^{p+(m-1-p)}} = (w^{2^p})^{2^{m-1-p}} = (1, 0)$, so $o(w) = 2^p$. But by Theorem 4.5, we have $o(a) \mid |K_n^*|$, so in particular we have $2^p \leq |K_n^*|$. Putting everything together, we get a contradiction $2^p \leq |K_n^*| \leq n^2 - 1 < M_p = 2^p - 1$.

6 Pocklington certificate

Pocklington certificate let us assess the primality of a number n by collecting enough factors of $n - 1$ and showing that these factors verify a given relation.

Theorem 6.1 (Pocklington) *If $F_1 > 1$, $R_1 > 0$ and $N - 1 = F_1 R_1$, if we have that for each prime number p such that $p \mid F_1$ there exists an a such that $a^{N-1} \equiv 1 [N]$ and $(a^{(N-1)/p} - 1)^\wedge N = 1$, then for each prime n such that $n \mid N$ we have $n \equiv 1 [F_1]$.*

To prove $n \equiv 1 [F_1]$, we show that $F_1 \mid n - 1$. It is enough to prove that $p^\alpha \mid n - 1$ for each prime number p such that $p^\alpha \mid F_1$. If $\alpha \geq 1$, we have $p \mid F_1$. So there exists a such that $a^{N-1} \equiv 1 [N]$ and $(a^{(N-1)/p} - 1)^\wedge N = 1$. We have $a \bmod n \in (\mathbb{Z}/n\mathbb{Z})^*$, so $o(a \bmod n)$ makes sense. We are going to prove that $p^\alpha \mid o(a \bmod n)$ which is enough since $o(a \bmod n) \mid n - 1$ by Theorem 4.7. We have $n \mid N$, so $a^{N-1} \equiv 1 [N]$ implies $(a \bmod n)^{N-1} \equiv 1 [n]$. By Theorem 4.2 we get $o(a \bmod n) \mid N - 1$. We have also $(a^{(N-1)/p} - 1)^\wedge N = 1$, so in particular as $n \mid N$ we have $(a^{(N-1)/p} - 1)^\wedge n = 1$. If we had $o(a \bmod n) \mid (N - 1)/p$, by Theorem 4.2 we would get that $a^{(N-1)/p} \equiv 1 [n]$, so we would have $n = (a^{(N-1)/p} - 1)^\wedge n$. To sum up, we have that $o(a \bmod n) \mid N - 1$ but also that $o(a \bmod n) \nmid (N - 1)/p$. This means that $o(a \bmod n)$ contains all the power of p , i.e. for all β such that $p^\beta \mid N - 1$ we have $p^\beta \mid o(a \bmod n)$. So we get that $p^\alpha \mid o(a \bmod n)$.

Theorem 6.2 *If $F_1 > 1$, $F_1 \mid N - 1$ and $F_1 > N$, if we have that for each prime number p such that $p \mid F_1$ there exists an a such that $a^{N-1} \equiv 1 [N]$ and $(a^{(N-1)/p} - 1)^\wedge N = 1$, then N is prime.*

This is a direct corollary of Theorem 6.1. If N was composite, there would be an n such that $1 < n \leq \sqrt{N}$ and $n \mid N$. We have $n \leq \sqrt{N} < F_1$ and by Theorem 6.1 we also have $n \equiv 1 [F_1]$. So we deduce that $n = 1$ which contradicts $1 < n$.

Now we can derive two usual tests from this last corollary.

Definition 6.1 (Fermat numbers) F_p is the p th Fermat number if $F_p = 2^{2^p} - 1$.

Theorem 6.3 (Pepin Test) *If $p > 1$ and $3^{(F_p-1)/2} \equiv -1 [F_p]$ then F_p is prime.*

This is a direct application of Theorem 6.2 with $a = 3$ and $F_1 = 2^{2^p}$.

Theorem 6.4 (Proth Test) *If $p = h2^k + 1$ with $2^k > h$ and there exists an a such that $a^{(n-1)/2} \equiv -1 \pmod{p}$ then p is prime.*

This is a direct application of Theorem 6.2 with $F_1 = 2^k$.

Theorem 6.2 requires to be able to factorize $N - 1$ till \sqrt{N} . We can do considerably better ($\sqrt[3]{N/2}$ instead of \sqrt{N}) with the following theorem.

Theorem 6.5 *Let $F_1 > 1$, $R_1 > 0$ and $N - 1 = F_1 R_1$, such that F_1 is even and R_1 is odd, let $m \geq 1$, $s := R_1 / (2F_1)$, $r = R_1 \bmod (2F_1)$ such that $N < (mF_1 + 1) * (2F_1^2 + (r - m)F_1 + 1)$ and for all λ such that $1 \leq \lambda < m$, we have $(\lambda F_1 + 1) \nmid N$, if for each prime number p such that $p \mid F_1$ there exists an a such that $a^{N-1} \equiv 1 \pmod{N}$ and $(a^{(N-1)/p} - 1)^N = 1$, then if $s = 0$ or $r^2 - 8s$ is not a square then N is prime.*

We proceed by contradiction. Suppose that N is composite, we are going to prove that $s \neq 0$ and $r^2 - 8s$ is a square. N is composite, so there exist K_1, K_2 such that $N = K_1 K_2$. By Theorem 6.1 we know that $K_i \equiv 1 \pmod{F_1}$. So there exist c, d such that $N = (cF_1 + 1)(dF_1 + 1)$. Furthermore the fact that for all λ such that $1 \leq \lambda < m$, we have $(\lambda F_1 + 1) \nmid N$ gives us that $c \geq m$ and $d \geq m$. We have $N - 1 = F_1 R_1$ and $N = cdF_1^2 + (c + d)F_1 + 1$ so $R_1 = cdF_1 + (c + d)$. We have also that R_1 is odd and F_1 is even, so cdF_1 is even which implies that $c + d$ is odd. So cd must be even. We have $R_1 = (cd/2)2F_1 + (c + d)$ and by definition of s and r we have also $R_1 = s2F_1 + r$. If we manage to prove that $c + d = r$ we are done since $s = (cd/2) \neq 0$ and $r^2 - 8s = (c + d)^2 - 4cd = (c - d)^2$.

To prove $c + d = r$, as we have $(cd/2)2F_1 + (c + d) = s2F_1 + r$ and $r = R_1 \bmod (2F_1)$ we know that $r = c + d \bmod (2F_1)$, we then just need to prove that $(c + d) - r < 2F_1$ to conclude. We have

$$(mF_1 + 1) * (2F_1^2 + (r - m)F_1 + 1) > N = cdF_1^2 + (c + d)F_1 + 1$$

We have $(c - m)(d - m) \geq 0$, so $cd \geq m(c + d) - m^2$. Using this inequality to minor the right side of the previous equation we get:

$$\begin{aligned} (mF_1 + 1) * (2F_1^2 + (r - m)F_1 + 1) &> (m(c + d) - m^2)F_1^2 + (c + d)F_1 + 1 \\ &= (mF_1 + 1)((c + d) - m)F_1 + 1 \end{aligned}$$

Simplifying we get $2F_1^2 + (r - m)F_1 + 1 > ((c + d) - m)F_1 + 1$ so $(c + d) - r < 2F_1$.

7 Acknowledgments

This formalisation has been mainly motivated by Benjamin Gregoire’s quest for large prime numbers verified by COQ.

Proofs of Sections 5 and 6 are transcriptions from the beautiful site <http://primes.utm.edu/prove>. Proofs of Theorems 6.5 and 6.1 are transcriptions of the seminal paper [1].

References

- [1] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. 29:620–647, 1975.