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

and the functions are:

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

1.2 Lists

Lists are denoted as $[\mathbf{a}_1;\mathbf{a}_2;::::;\mathbf{a}_n]$. We write the size of a list $\mathbf{L}$ as $|\mathbf{L}|$, the concatenation of two lists $\mathbf{L}_1$, $\mathbf{L}_2$ as $\mathbf{L}_1 + \mathbf{L}_2$ and the fact that an element $\mathbf{a}$ belongs to a list $\mathbf{L}$ as $\mathbf{a} \in \mathbf{L}$.

1.3 Sets

Sets are denoted as $\{\mathbf{a}_1;\mathbf{a}_2;::::;\mathbf{a}_n\}$. We write the size of a set $\mathbf{G}$ as $|\mathbf{G}|$, the fact that an element $\mathbf{a}$ belongs to a set $\mathbf{G}$ as $\mathbf{a} \in \mathbf{G}$, the fact that a set $\mathbf{G}_1$ is included in a set $\mathbf{G}_2$ as $\mathbf{G}_1 \subset \mathbf{G}_2$. Over sets, we define the notions of finite monoid and finite group:

- **Finite Monoid**: $(\mathbf{G};*)$ is a finite monoid, iff

  $\mathbf{G}$ is finite: $\mathbf{G} = \{\mathbf{e};\mathbf{a}_1;\mathbf{a}_2;:::;\mathbf{a}_n\}$,
  the operation $*$ is internal: if $\mathbf{a} \in \mathbf{G}$ and $\mathbf{b} \in \mathbf{G}$ then $\mathbf{ab} \in \mathbf{G}$,
  the operation $*$ is associative: $\mathbf{a}(\mathbf{bc}) = (\mathbf{ab})\mathbf{c}$,
  the element $\mathbf{e}$ is neutral: $\mathbf{ea} = \mathbf{a} = \mathbf{ae}$.

- **Finite Group**: $(\mathbf{G};*)$ is a finite group, iff

  $\mathbf{G}$ is finite: $\mathbf{G} = \{\mathbf{e};\mathbf{a}_1;\mathbf{a}_2;:::;\mathbf{a}_n\}$,
  the operation $*$ is internal: if $\mathbf{a} \in \mathbf{G}$ and $\mathbf{b} \in \mathbf{G}$ then $\mathbf{ab} \in \mathbf{G}$,
  the operation $*$ is associative: $\mathbf{a}(\mathbf{bc}) = (\mathbf{ab})\mathbf{c}$,
  the element $\mathbf{e}$ is neutral: $\mathbf{ea} = \mathbf{a} = \mathbf{ae}$,
  every element has an inverse: $\mathbf{aa}^{-1} = \mathbf{e} = \mathbf{a}^{-1}\mathbf{a}$.

A group $(\mathbf{H};*)$ is a subgroup of a group $(\mathbf{G};*)$ if $\mathbf{G} \subset \mathbf{H}$.

2 Basic Theorems

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

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

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 substraction: if $\mathbf{m} \mid \mathbf{n}$ and $\mathbf{m} \mid \mathbf{p}$ then $\mathbf{m} \mid \mathbf{n} - \mathbf{p}$. Now, we have the hypothesis $\mathbf{m} \mid \mathbf{np}$ and we also have that $\mathbf{m} \mid \mathbf{mp}$. Remembering Euclid algorithm and using the compatibility of the substraction we can derive that $\mathbf{m} \mid (\mathbf{m} \hat{} \mathbf{n})\mathbf{p}$. As we have *coprime*$(\mathbf{m};\mathbf{n})$, we get the expected result $\mathbf{m} \mid \mathbf{p}$.

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

Once again the proof of this theorem follows Euclid algorithm to compute the gcd of $\mathbf{m}$ and $\mathbf{n}$.

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

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

Theorem 2.4 (Lagrange) *If* $(\mathbf{H};*)$ *is a subground of* $(\mathbf{G};*)$ *then* $|\mathbf{H}| \,|\, |\mathbf{G}|$.

Let $\mathbf{H} = \{\mathbf{e};\mathbf{a}_1;\mathbf{a}_2;\ldots;\mathbf{a}_n\}$ and $\mathbf{G} = \{\mathbf{e};\mathbf{b}_1;\mathbf{b}_2;\ldots;\mathbf{b}_m\}$, we have $\mathbf{H} \subset \mathbf{G}$. We build the increasing sequence $(\mathbf{L}_i)_{i \leq m}$ of lists as follows:

$\mathbf{L}_0 = [\mathbf{e};\mathbf{a}_1;\mathbf{a}_2 :: \mathbf{a}_n]$;

if $\mathbf{b}_{i+1} \in \mathbf{L}_i$, $\mathbf{L}_{i+1} = \mathbf{L}_i$;

if $\mathbf{b}_{i+1} \notin \mathbf{L}_i$, $\mathbf{L}_{i+1} = [\mathbf{b}_{i+1}\mathbf{e};\mathbf{b}_{i+1}\mathbf{a}_1;\mathbf{b}_{i+1}\mathbf{a}_2;\ldots;\mathbf{b}_{i+1}\mathbf{a}_n] + \mathbf{L}_i$.

We use the convention that $\mathbf{a}_0 = \mathbf{e}$ and $\mathbf{b}_0 = \mathbf{e}$. It is easy to show that for all $\mathbf{i} \leq \mathbf{m}$ we have $|\mathbf{H}| \,|\, |\mathbf{L}_i|$ and $\mathbf{b}_i \in \mathbf{L}_m$. We are left with proving that $|\mathbf{L}_m| = |\mathbf{H}_m|$. To do so, we just need to show that the elements of $\mathbf{H}$ occurs only once in $\mathbf{L}_m$. By contradiction, suppose $\mathbf{b}_k$ occurs more than once in $\mathbf{L}_m$. There are two possibilities: either there exists $\mathbf{i}$ such that $\mathbf{b}_k$ occurs more than

once in $\mathbf{L}_i$ but not in $\mathbf{L}_{i-1}$[1], or $\mathbf{b}_k$ occurs in $\mathbf{L}_i$ and $\mathbf{L}_i - \mathbf{L}_{i-1}$. In the first case, there exist $\mathbf{u}$ and $\mathbf{v}$, $\mathbf{b}_i\mathbf{a}_u = \mathbf{b}_k = \mathbf{b}_i\mathbf{a}_v$. Simplifying by $\mathbf{b}_i^{-1}$, we get $\mathbf{a}_u = \mathbf{a}_v$. So as $\mathbf{G}$ is a set, we have $\mathbf{u} = \mathbf{v}$. This contradicts the fact that $\mathbf{b}_k$ occurs more than once in $\mathbf{L}_i$. In the second case, there exist $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{j}$ with $\mathbf{j} < \mathbf{i}$ such that $\mathbf{b}_i\mathbf{a}_u = \mathbf{b}_k = \mathbf{b}_j\mathbf{a}_v$. Simplifying by $\mathbf{a}_u^{-1}$, we get $\mathbf{b}_i = \mathbf{b}_j(\mathbf{a}_v\mathbf{a}_u^{-1})$. As $\mathbf{a}_v \in \mathbf{G}$ and $\mathbf{a}_u \in \mathbf{G}$, there exists a $\mathbf{l}$ such that $\mathbf{b}_i = \mathbf{b}_j\mathbf{a}_l$, so $\mathbf{b}_i \in \mathbf{L}_j$. This contradicts the fact that $\mathbf{b}_i \notin \mathbf{L}_{i-1}$ that is true by construction since $\mathbf{L}_i \neq \mathbf{L}_{i-1}$.

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

Theorem 3.1 *Let* $(\mathbf{G}; *)$ *be a finite monoid,* $(\mathbf{I}(\mathbf{G}); *)$ *is a finite subgroup.*

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

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

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

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

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

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

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

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

This is a direct consequence of Theorems 3.2 and 3.1.

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

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

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

This is a direct consequence of Theorems 2.3 and 3.4.

4 Order of an element

Given an element $\mathbf{a}$ of a group, we can construct a subgroup by repetitively multiplying $\mathbf{a}$ 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* $(\mathbf{G}; *)$ *be a finite group and* $\mathbf{a}$ *an element of* $\mathbf{G}$*, we define* $\mathbf{H}_a = \{\mathbf{a}^i | \mathbf{i} \in \mathbb{N}\}$,

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

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

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

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

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

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

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

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

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

Theorem 4.4 *Let* $(\mathbf{G};*)$ *be a finite group and* $\mathbf{a}$ *an element of* $\mathbf{G}$, $(\mathbf{H}_a;*)$ *is a finite subgroup of* $(\mathbf{G};*)$.

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

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

This is a direct consequence of Theorem 2.4 and $|\mathbf{H}_a| = \mathbf{o}(\mathbf{a})$.

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

This is a direct consequence of Theorems 4.5 and 3.4.

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

This is a direct consequence of Theorems 4.5 and 3.5

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

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

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

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* $\mathbf{n}$ *be a number, we define* $\mathbf{K}_n$ *as* $(\mathbb{Z}/\mathbf{n}\mathbb{Z})^2$*, i.e.* $\mathbf{K}_n = \{(\mathbf{a};\mathbf{b}) \,|\, 0 \leq \mathbf{a} \leq \mathbf{n} \text{ and } 0 \leq \mathbf{b} \leq \mathbf{n}\}$.

Definition 5.2 *we define the operation* $\oplus$ *as* $(\mathbf{a}_1;\mathbf{b}_1) \oplus (\mathbf{a}_2;\mathbf{b}_2) = ((\mathbf{a}_1 + \mathbf{b}_1) \bmod \mathbf{n};(\mathbf{b}_1 + \mathbf{b}_n) \bmod \mathbf{n})$.

Definition 5.3 *we define the operation* $\odot$ *as* $(\mathbf{a}_1;\mathbf{b}_1) \odot (\mathbf{a}_2;\mathbf{b}_2) = ((\mathbf{a}_1\mathbf{a}_2 + 3\mathbf{b}_1\mathbf{b}_2) \bmod \mathbf{n};(\mathbf{a}_1\mathbf{b}_2 + \mathbf{a}_2\mathbf{b}_1) \bmod \mathbf{n})$.

Definition 5.4 *we define the power as* $(\mathbf{a};\mathbf{b})^n = \underbrace{(\mathbf{a};\mathbf{b}) \odot (\mathbf{a};\mathbf{b}) \odot \cdots \odot (\mathbf{a};\mathbf{b})}_{n}$.

Definition 5.5 *For* $\mathbf{n} > 1$*, we define two elements of* $\mathbf{K}_n$ $\mathbf{w}$ *as* $(2;1)$*,* $\mathbf{v}$ *as* $(2;\mathbf{n}-1)$ *and we define the sequence* $(\mathbf{S}_m)_{m\in\mathbb{N}}$ *over the natural numbers such that* $\mathbf{S}_0 = 4$ *and* $\mathbf{S}_{m+1} = \mathbf{S}_m^2 - 2$.

Theorem 5.1 *For* $\mathbf{n} > 1$*, we have* $\mathbf{w} \odot \mathbf{v} = (1;0)$,

We have

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

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

We prove this by induction.
If $\mathbf{m} = 1$, we have $\mathbf{w} + \mathbf{v} = (2;1) \oplus (2;\mathbf{n}-1) = (4 \bmod \mathbf{n};\mathbf{n} \bmod \mathbf{n}) = (4 \bmod \mathbf{n};0)$.

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

$$(\mathbf{w}^{2^{m-1}} \oplus \mathbf{v}^{2^{m-1}}) \odot (\mathbf{w}^{2^{m-1}} \oplus \mathbf{v}^{2^{m-1}}) = (\mathbf{S}_m \bmod \mathbf{n}; 0) \odot (\mathbf{S}_m \bmod \mathbf{n}; 0)$$

Using the distributivity, commutativity and associativity gives us

$$(\mathbf{w}^{2^m} \oplus \mathbf{v}^{2^m}) \oplus (2; 0) \odot (\mathbf{w}^{2^{m-1}} \mathbf{v}^{2^{m-1}}) = (\mathbf{S}_m^2 \bmod \mathbf{n}; 0)$$

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

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

For the right side, using Definition 5.5 we get:

$$(\mathbf{S}_m^2 \bmod \mathbf{n}; 0) = ((\mathbf{S}_{m+1} + 2) \bmod \mathbf{n}; 0) = (\mathbf{S}_{m+1} \bmod \mathbf{n}; 0) \oplus (2; 0)$$

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

$$(\mathbf{w}^{2^m} \oplus \mathbf{v}^{2^m}) = (\mathbf{S}_{m+1} \bmod \mathbf{n}; 0)$$

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

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

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

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

Definition 5.6 (Mersenne numbers) $\mathbf{M}_p$ *is the pth Mersenne if* $\mathbf{M}_p = 2^p - 1$*.*

Theorem 5.4 (Lucas-Lehmer Test) *If* $\mathbf{p} > 2$ *and* $\mathbf{M}_p \,|\, \mathbf{S}_{p-1}$ *then* $\mathbf{M}_p$ *is prime.*

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

6 Pocklington certificate

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

Theorem 6.1 (Pocklington) *If* $\mathbf{F}_1 > 1$, $\mathbf{R}_1 > 0$ *and* $\mathbf{N} - 1 = \mathbf{F}_1\mathbf{R}_1$, *if we have that for each prime number* $\mathbf{p}$ *such that* $\mathbf{p} \,|\, \mathbf{F}_1$ *there exists an* $\mathbf{a}$ *such that* $\mathbf{a}^{N-1} \equiv 1\,[\mathbf{N}]$ *and* $(\mathbf{a}^{(N-1)/p} - 1) \hat{} \mathbf{N} = 1$, *then for each prime* $\mathbf{n}$ *such that* $\mathbf{n} \,|\, \mathbf{N}$ *we have* $\mathbf{n} \equiv 1\,[\mathbf{F}_1]$.

To prove $\mathbf{n} \equiv 1\,[\mathbf{F}_1]$, we show that $\mathbf{F}_1 \,|\, \mathbf{n} - 1$. It is enough to prove that $\mathbf{p}^\alpha \,|\, \mathbf{n} - 1$ for each prime number $\mathbf{p}$ such that $\mathbf{p}^\alpha \,|\, \mathbf{F}_1$. If ≥ 1, we have $\mathbf{p} \,|\, \mathbf{F}_1$. So there exists $\mathbf{a}$ such that $\mathbf{a}^{N-1} \equiv 1\,[\mathbf{N}]$ and $(\mathbf{a}^{(N-1)/p} - 1) \hat{} \mathbf{N} = 1$. We have $\mathbf{a} \bmod \mathbf{n} \in (\mathbb{Z}/\mathbf{n}\mathbb{Z})^*$, so $\mathbf{o}(\mathbf{a} \bmod \mathbf{n})$ makes sense. We are going to prove that $\mathbf{p}^\alpha \,|\, \mathbf{o}(\mathbf{a} \bmod \mathbf{n})$ which is enough since $\mathbf{o}(\mathbf{a} \bmod \mathbf{n}) \,|\, \mathbf{n} - 1$ by Theorem 4.7. We have $\mathbf{n} \,|\, \mathbf{N}$, so $\mathbf{a}^{N-1} \equiv 1\,[\mathbf{N}]$ implies $(\mathbf{a} \bmod \mathbf{n})^{N-1} \equiv 1\,[\mathbf{n}]$. By Theorem 4.2 we get $\mathbf{o}(\mathbf{a} \bmod \mathbf{n}) \,|\, \mathbf{N} - 1$. We have also $(\mathbf{a}^{(N-1)/p} - 1) \hat{} \mathbf{N} = 1$, so in particular as $\mathbf{n} \,|\, \mathbf{N}$ we have $(\mathbf{a}^{(N-1)/p} - 1) \hat{} \mathbf{n} = 1$. If we had $\mathbf{o}(\mathbf{a} \bmod \mathbf{n}) \,|\, (\mathbf{N} - 1)/\mathbf{p}$, by Theorem 4.2 we would get that $\mathbf{a}^{(N-1)/p} \equiv 1\,[\mathbf{n}]$, so we would have $\mathbf{n} = (\mathbf{a}^{(N-1)/p} - 1) \hat{} \mathbf{n}$. To sum up, we have that $\mathbf{o}(\mathbf{a} \bmod \mathbf{n}) \,|\, \mathbf{N} - 1$ but also that $\mathbf{o}(\mathbf{a} \bmod \mathbf{n}) \not| (\mathbf{N} - 1)/\mathbf{p}$. This means that $\mathbf{o}(\mathbf{a} \bmod \mathbf{n})$ contains all the power of $\mathbf{p}$, i.e. for all such that $\mathbf{p}^\beta \,|\, \mathbf{N} - 1$ we have $\mathbf{p}^\beta \,|\, \mathbf{o}(\mathbf{a} \bmod \mathbf{n})$. So we get that $\mathbf{p}^\alpha \,|\, \mathbf{o}(\mathbf{a} \bmod \mathbf{n})$.

Theorem 6.2 *If* $\mathbf{F}_1 > 1$, $\mathbf{F}_1 \mid \mathbf{N} - 1$ *and* $\mathbf{F}_1 > \sqrt{\mathbf{N}}$, *if we have that for each prime number* $\mathbf{p}$ *such that* $\mathbf{p} \mid \mathbf{F}_1$ *there exists an* $\mathbf{a}$ *such that* $\mathbf{a}^{N-1} \equiv 1\,[\mathbf{N}]$ *and* $(\mathbf{a}^{(N-1)/p} - 1) \hat{} \mathbf{N} = 1$, *then* $\mathbf{N}$ *is prime.*

This is a direct corollary of Theorem 6.1. If $\mathbf{N}$ was composite, there would be an $\mathbf{n}$ such that $1 < \mathbf{n} \leq \sqrt{\mathbf{N}}$ and $\mathbf{n} \mid \mathbf{N}$. We have $\mathbf{n} \leq \sqrt{\mathbf{N}} < \mathbf{F}_1$ and by Theorem 6.1 we also have $\mathbf{n} \equiv 1\,[\mathbf{F}_1]$. So we deduce that $\mathbf{n} = 1$ which contradicts $1 < \mathbf{n}$.

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

Definition 6.1 (Fermat numbers) $\mathbf{F}_p$ *is the pth Fermat number if* $\mathbf{F}_p = 2^{2^p} - 1$.

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

This is a direct application of Theorem 6.2 with $\mathbf{a} = 3$ and $\mathbf{F}_1 = 2^{2^p}$.

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

This is a direct application of Theorem 6.2 with $\mathbf{F}_1 = 2^k$.

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

Theorem 6.5 *Let* $\mathbf{F}_1 > 1$, $\mathbf{R}_1 > 0$ *and* $\mathbf{N} - 1 = \mathbf{F}_1\mathbf{R}_1$, *such that* $\mathbf{F}_1$ *is even and* $\mathbf{R}_1$ *is odd, let* $\mathbf{m} \geq 1$, $\mathbf{s} := \mathbf{R}_1 = (2\mathbf{F}_1)$, $\mathbf{r} = \mathbf{R}_1 \bmod (2\mathbf{F}_1)$ *such that* $\mathbf{N} < (\mathbf{m}\mathbf{F}_1 + 1) * (2\mathbf{F}_1^2 + (\mathbf{r} - \mathbf{m})\mathbf{F}_1 + 1)$ *and for all such that* $1 \leq < \mathbf{m}$, *we have* $(\mathbf{F}_1 + 1) \not| \mathbf{N}$, *if for each prime number* $\mathbf{p}$ *such that* $\mathbf{p} \mid \mathbf{F}_1$ *there exists an* $\mathbf{a}$ *such that* $\mathbf{a}^{N-1} \equiv 1\,[\mathbf{N}]$ *and* $(\mathbf{a}^{(N-1)/p} - 1) \hat{} \mathbf{N} = 1$, *then if* $\mathbf{s} = 0$ *or* $\mathbf{r}^2 - 8\mathbf{s}$ *is not a square then* $\mathbf{N}$ *is prime.*

We proceed by contradiction. Suppose that $\mathbf{N}$ is composite, we are going to prove that $\mathbf{s} \neq 0$ and $\mathbf{r}^2 - 8\mathbf{s}$ is a square. $\mathbf{N}$ is composite, so there exist $\mathbf{K}_1$, $\mathbf{K}_2$ such that $\mathbf{N} = \mathbf{K}_1\mathbf{K}_2$. By Theorem 6.1 we know that $\mathbf{K}_i \equiv 1\,[\mathbf{F}_1]$. So there exist $\mathbf{c}$, $\mathbf{d}$ such that $\mathbf{N} = (\mathbf{c}\mathbf{F}_1 + 1)(\mathbf{d}\mathbf{F}_1 + 1)$. Furthermore the fact that for all such that $1 \leq < \mathbf{m}$, we have $(\mathbf{F}_1 + 1) \not| \mathbf{N}$ gives us that $\mathbf{c} \geq \mathbf{m}$ and $\mathbf{d} \geq \mathbf{m}$. We have $\mathbf{N} - 1 = \mathbf{F}_1\mathbf{R}_1$ and $\mathbf{N} = \mathbf{c}\mathbf{d}\mathbf{F}_1^2 + (\mathbf{c} + \mathbf{d})\mathbf{F}_1 + 1$ so $\mathbf{R}_1 = \mathbf{c}\mathbf{d}\mathbf{F}_1 + (\mathbf{c} + \mathbf{d})$. We have also that $\mathbf{R}_1$ is odd and $\mathbf{F}_1$ is even, so $\mathbf{c}\mathbf{d}\mathbf{F}_1$ is even which implies that $\mathbf{c} + \mathbf{d}$ is odd. So $\mathbf{c}\mathbf{d}$ must be even. We

have $\mathbf{R}_1 = (\mathbf{cd}{=}2)2\mathbf{F}_1 + (\mathbf{c}+\mathbf{d})$ and by definition of $\mathbf{s}$ and $\mathbf{r}$ we have also $\mathbf{R}_1 = \mathbf{s}2\mathbf{F}_1 + \mathbf{r}$. If we manage to prove that $\mathbf{c}+\mathbf{d} = \mathbf{r}$ we are done since $\mathbf{s} = (\mathbf{cd}{=}2) \neq 0$ and $\mathbf{r}^2 - 8\mathbf{s} = (\mathbf{c}+\mathbf{d})^2 - 4\mathbf{cd} = (\mathbf{c}-\mathbf{d})^2$.

To prove $\mathbf{c}+\mathbf{d} = \mathbf{r}$, as we have $(\mathbf{cd}{=}2)2\mathbf{F}_1 + (\mathbf{c}+\mathbf{d}) = \mathbf{s}2\mathbf{F}_1 + \mathbf{r}$ and $\mathbf{r} = \mathbf{R}_1 \mod (2\mathbf{F}_1)$ we know that $\mathbf{r} = \mathbf{c}+\mathbf{d} \mod (2\mathbf{F}_1)$, we then just need to prove that $(\mathbf{c}+\mathbf{d}) - \mathbf{r} < 2\mathbf{F}_1$ to conclude. We have

$$(\mathbf{mF}_1 + 1) * (2\mathbf{F}_1^2 + (\mathbf{r}-\mathbf{m})\mathbf{F}_1 + 1) > \mathbf{N} = \mathbf{cdF}_1^2 + (\mathbf{c}+\mathbf{d})\mathbf{F}_1 + 1$$

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

$$\begin{aligned}(\mathbf{mF}_1 + 1) * (2\mathbf{F}_1^2 + (\mathbf{r}-\mathbf{m})\mathbf{F}_1 + 1) &> (\mathbf{m}(\mathbf{c}+\mathbf{d}) - \mathbf{m}^2)\mathbf{F}_1^2 + (\mathbf{c}+\mathbf{d})\mathbf{F}_1 + 1 \\ &= (\mathbf{mF}_1 + 1)(((\mathbf{c}+\mathbf{d}) - \mathbf{m})\mathbf{F}_1 + 1)\end{aligned}$$

Simplifying we get $2\mathbf{F}_1^2 + (\mathbf{r}-\mathbf{m})\mathbf{F}_1 + 1 > ((\mathbf{c}+\mathbf{d})-\mathbf{m})\mathbf{F}_1 + 1$ so $(\mathbf{c}+\mathbf{d})-\mathbf{r} < 2\mathbf{F}_1$.

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.