1 Lucas–Lehmer Theorem

Let n be a natural number and $M_n := 2^n - 1$. The primality of M_n implies the primality of n.

Hence, for a given prime number n we set

$$\begin{aligned} s_0 &:= 4 \\ s_{k+1} &:= s_k^2 - 2 \qquad k = 0, 1, 2, \ldots, n-2 \end{aligned} \tag{1}$$

The series s is called the LL-series.

Now M_n is prime $\iff M_n \mid s_n - 2$.

1.1 Proof.

Let $n \geq 3$ and $M_n = 2^n - 1$ be primes. Let $T := \mathbb{Z}[\sqrt{3}]$, then $T \ni \psi := 2 + \sqrt{3}$ and $T \ni \bar{\psi} := 2 - \sqrt{3}$. One easily sees

$$\psi\bar{\psi} = 1 \tag{2}$$

Especially we see $M_n \equiv 7 \bmod 8$. From the quadratic reciprocity theorem we know 3 is not a quadratic remainder of M_n.

By induction it can easily be seen that the elements of the LL-series suffice:

$$s_{n-2} = \psi^{2^{n-2}} + \bar{\psi}^{2^{n-2}} = \bar{\psi}^{2^{n-2}}(1 + \psi^{2^{n-1}}) \tag{3}$$

"⇒" To show $M_n \mid s_{n-2}$, it is enough to show

$$\psi^{2^{n-1}} \equiv -1 \bmod M_n \tag{4}$$

(with equation (3)).

Using

$$2^{n-1} = (M_n + 1)/2$$

and

$$2^{(M_n-1)/2} \equiv 1 \bmod M_n$$

we get

$$\begin{aligned} \psi^{2^{n-1}} &\equiv 2^{(M_n-1)/2}\left(\frac{1+\sqrt{3}}{x}\right)^{M_n+1} \\ &\equiv \frac{1+\sqrt{3}}{2}(1+\sqrt{3})^{M_n} \\ &\equiv \frac{1+\sqrt{3}}{2}(1-\sqrt{3}) \\ &\equiv -1 \bmod M_n \end{aligned} \tag{5}$$

"⇐" Suppose $M_n \mid s_{n-2}$ (in $\mathbb{Z}$).

Then also $M_n \mid \psi^{2^{n-2}} s_{n-2}$ (in T).

Hence $1 + \psi^{2^{n-1}} \equiv 0 \bmod M_n$, thus

$$\psi^{2^n} \equiv 1 \bmod M_n \tag{6}$$

Let q be an arbitrary prime factor of M_n. (note $q \neq 2$ and $q \neq 3$)

Then from equation (6) it follows that $\psi^{2^n} \equiv 1 \bmod q$.

Note $2^n = \operatorname{ord}\psi$ in the multiplicative group $T_q := \{a + b\sqrt{3} : 0 \leq a, b < q,\ a + b > 0\}$. From k being an exponent of ψ in T_q (i.e. $\psi^k \equiv 1 \bmod q$) it follows that $2^n \mid k$.

Now we use this result to show that M_n equals the chosen prime q.

From the quadratic reciprocity theorem we know that we have two cases to consider:

1. $\sqrt{3}$ is a square in T_q:

$$\begin{aligned} \psi^{q-1} &\equiv (2 - \sqrt{3})(2 + \sqrt{3})^q && \text{see equation (2)} \\ &\equiv ((2 - \sqrt{3})(2 + \sqrt{3}) && \text{see quad. reci. thm.} \\ &\equiv 1 \bmod q \end{aligned} \tag{7}$$

   From the preliminaries we see $2^n \mid q - 1$, thus let $2^n h = q - 1$ with $h \geq 1$. But then it follows

$$q = 2^n h + 1 > 2^n - 1 = M_n \tag{8}$$

   contradicting the fact $q \mid M_n$. Thus this case does not occur.

2. $\sqrt{3}$ is not a square in T_q:

$$\begin{aligned} \psi^{q+1} &\equiv (2 + \sqrt{3})(2 + \sqrt{3})^q \\ &\equiv (2 + \sqrt{3})(2 - \sqrt{3}) && \text{see quad. reci. thm.} \\ &\equiv 1 \end{aligned} \tag{9}$$

   From the preliminaries we see now that $q + 1$ is a multiple of 2^n, thus let $2^n h = q + 1$ with $h \geq 1$.
   Now it results in

$$q = 2^n h - 1 \geq 2^n - 1 = M_n \tag{10}$$

   Since q was chosen as divisor of M_n, it follows $h = 1$ and thus $q = M_n$.
   As q is prime, so is M_n.

$\square$