A LLT-like test for proving the primality of Fermat numbers.

1 Another proof by R. Gerbicz

I've found a proof in my number theory book for standard Lucas-Lehmer test for Mersenne numbers. Proof isn't using theorems for Lucas sequences. I modified this proof to give an easy and another proof for your theorem! So I'm almost sure that your theorem is true:

Theorem 1 (R. Gerbicz) *Let $n \geq 1$ then F_n is prime if and only if it divides S_{2^n-2} where $S_0 = 5$ and $S_{k+1} = S_k^2 - 2$.*

By induction it is easy to prove, that: $S_k = \left(\frac{5+\sqrt{21}}{2}\right)^{2^k} + \left(\frac{5-\sqrt{21}}{2}\right)^{2^k}$
From this:

$$S_{2^n-2} = \left(\frac{5+\sqrt{21}}{2}\right)^{(F_n-1)/4} + \left(\frac{5-\sqrt{21}}{2}\right)^{(F_n-1)/4}$$

But: $\frac{5+\sqrt{21}}{2} * \frac{5-\sqrt{21}}{2} = 1$, using this:

$$S_{2^n-2} = \left(\frac{5-\sqrt{21}}{2}\right)^{(F_n-1)/4} * \left(\left(\frac{5+\sqrt{21}}{2}\right)^{(F_n-1)/2} + 1\right)$$

Multiply this equation by $2^{3*(F_n-1)/4}$, we get:

$$2^{3*(F_n-1)/4} * S_{2^n-2} = (5-\sqrt{21})^{(F_n-1)/4} * ((5+\sqrt{21})^{(F_n-1)/2} + 2^{(F_n-1)/2})$$

So S_{2^n-2} is divisible by F_n if and only if $2^{3*(F_n-1)/4} * S_{2^n-2}$ is divisible by F_n, because F_n is odd. And the right side of equation is divisible by F_n if and only if $(5+\sqrt{21})^{(F_n-1)/2} + 2^{(F_n-1)/2}$ is divisible by F_n because $(5-\sqrt{21})/2$ is unit in $Q[\sqrt{21}]$ (because $\frac{5-\sqrt{21}}{2} * \frac{5+\sqrt{21}}{2} = 1$), so $gcd(5+\sqrt{21}, F_n)$ is 1 or 2, but F_n is odd, so they are relative primes, it means that F_n divides $(5+\sqrt{21})^{(F_n-1)/2} + 2^{(F_n-1)/2}$ in $Q[\sqrt{21}]$.

So S_{2^n-2} is divisible by F_n (in Z) if and only if $(5+\sqrt{21})^{(F_n-1)/2} + 2^{(F_n-1)/2}$ is divisible by F_n in $Q[\sqrt{21}]$.

Lemma: if $q > 2$ is prime, where $gcd(21, q) = 1$ and a,b are integers, then $(a+b\sqrt{21})^q \equiv a + ({}^{21}/_{q})b\sqrt{21} \pmod{q}$ in $Q[\sqrt{21}]$.

Proof: by binomial theorem we can expand the power, but $binomial(q, k) \equiv 0 \pmod{q}$, if $0 < k < q$, so we can get (using also little-Fermat theorem in Z): $(a+b\sqrt{21})^q \equiv a^q + b^q\sqrt{21}^q \equiv a + b\sqrt{21} * 21^{(q-1)/2} \equiv a + b\sqrt{21}({}^{21}\!/\!_{q}) \pmod q$, what is needed.

First I prove that if $(5+\sqrt{21})^{(F_n-1)/2} + 2^{(F_n-1)/2}$ is divisible by F_n in $Q[\sqrt{21}]$ then F_n is prime !
So we know that $(5+\sqrt{21})^{(F_n-1)/2} + 2^{(F_n-1)/2} \equiv 0 \pmod{F_n}$ Dividing by $2^{(F_n-1)/2}$ and subtracting 1: $\left(\frac{5+\sqrt{21}}{2}\right)^{(F_n-1)/2} \equiv -1 \pmod{F_n}$; squaring this equation: $\left(\frac{5+\sqrt{21}}{2}\right)^{F_n-1} \equiv 1 \pmod{F_n}$.
Let q is a prime divisor of F_n then previous two equations are also true $\pmod q$ (because F_n is divisible by q) from these 2 equations we get that the order of $(5+\sqrt{21})/2 \mod q$ is $F_n - 1$.

First case: if $({}^{21}\!/\!_{q}) = 1$ then see $\left(\frac{5+\sqrt{21}}{2}\right)^{q-1} = \frac{5-\sqrt{21}}{2} * \left(\frac{5+\sqrt{21}}{2}\right)^{q} \equiv \frac{5-\sqrt{21}}{2} * \frac{(5+\sqrt{21})^q}{2} \equiv \frac{5-\sqrt{21}}{2} * \frac{5+\sqrt{21}}{2} \equiv 1 \pmod q$ (using lemma for $a=5; b=1$; and little-Fermat theorem in Z: $2^q \equiv 2 \pmod q$ in Z), so the order of $(5+\sqrt{21})/2$ is $\le q-1$,but we know that the order is $F_n - 1$, so $F_n - 1 \le q - 1$ from this $F_n \le q$, but q is a prime divisor of F_n so $F_n \ge q$ from these: $F_n = q$, so F_n is prime!

Second case: if $({}^{21}\!/\!_{q}) = -1$ Similar consider $\left(\frac{5+\sqrt{21}}{2}\right)^{q+1}$ this is $1 \mod q$ (you can prove this as in first case) so the order of $(5+\sqrt{21})/2$ is $\le q+1$ but the order is $F_n - 1$ so $F_n - 1 \le q + 1$ from this $q \ge F_n - 2$ but $q \le F_n$ is a prime divisor of F_n, so $F_n - 2 \le q \le F_n$ and q is a divisor; there is only one possible case: $q = F_n$, so F_n is prime. Proof is complete.

Now I prove that if $n \ge 1$ and F_n is prime then $(5+\sqrt{21})^{(F_n-1)/2} + 2^{(F_n-1)/2}$ is divisible by F_n in $Q[\sqrt{21}]$.

Proof: as you calculated: $Legendre3F_n = -1$ and $Legendre7F_n = -1$, so $Legendre21F_n = 1$.
You can check that: $6*(5+\sqrt{21}) = (3+\sqrt{21})^2$ take this equation up to the $(F_n-1)/2$-th power:

$$6^{(F_n-1)/2} * (5+\sqrt{21})^{(F_n-1)/2} = (3+\sqrt{21})^{F_n-1} \tag{1}$$

Here $3^{(F_n-1)/2} \equiv Legendre3F_n = -1 \pmod{F_n}$. We compute the right side of equation (1): $(3+\sqrt{21})^{F_n-1} = \frac{3-\sqrt{21}}{-12} * (3+\sqrt{21})^{F_n}$ because $(3-\sqrt{21})*(3+\sqrt{21}) = -12$; using lemma: $(3+\sqrt{21})^{F_n} \equiv 3 + Legendre21F_n\sqrt{21} = 3+\sqrt{21} \pmod{F_n}$. For lemma we used that F_n is prime. So $(3+\sqrt{21})^{F_n-1} \equiv \frac{3-\sqrt{21}}{-12} * (3+\sqrt{21}) \equiv 1 \pmod{F_n}$. We can write using equation (1) that $(-1)*2^{(F_n-1)/2}*(5+\sqrt{21})^{(F_n-1)/2} \equiv 1 \pmod{F_n}$. Multiply this equation by $2^{(F_n-1)/2}$ we get $(-1)*(5+\sqrt{21})^{(F_n-1)/2} \equiv 2^{(F_n-1)/2} \pmod{F_n}$, (we used that $2^{F_n-1} \equiv 1 \pmod{F_n}$) Add $(5+\sqrt{21})^{(F_n-1)/2}$ to previous equation:

$(5+\sqrt{21})^{(F_n-1)/2}+2^{(F_n-1)/2}\equiv 0 \pmod{F_n}$, what is required. Proof is complete. $\square$