PRIMALITY TEST FOR FERMAT NUMBERS USING QUARTIC RECURRENCE EQUATION

PREDRAG TERZICH

ABSTRACT. We present deterministic primality test for Fermat numbers , $F_n = 2^{2^n} + 1$, where $n \geq 2$. Essentially this test is similar to the Lucas-Lehmer primality test for Mersenne numbers.

1. INTRODUCTION.

Fermat numbers were first studied by Pierre de Fermat , who conjuctured that all Fermat numbers are prime. This conjecture was refuted by Leonhard Euler in 1732 when he showed that F_5 is composite . It is known that F_n is composite for $5 \leq n \leq 32$. Question,are there infinitely many Fermat primes is still an open problem . In 1856 Edouard Lucas has developed primality test for Mersenne numbers . Test was improved by Lucas in 1878 and Derrick Lehmer in 1930 s. The test uses a sequence S_i defined by $S_0 = 4$ and $S_{i+1} = {S_i}^2 - 2$ for $i \geq 1$. Mersenne number M_p is prime if and only if M_p divides S_{p-2} .

In this paper we give primality test for Fermat numbers using quartic recurrsive equation : $S_i = S_{i-1}^4 - 4S_{i-1}^2 + 2$. The test uses a sequence defined by this recursion .

2. THE TEST AND PROOF OF CORRECTNESS

2.1. **The test.** Let $F_n = 2^{2^n} + 1$ with $n \geq 2$. In pseudocode the test might be written :

//Determine if $F_n = 2^{2^n} + 1$ is prime
FermatPrime(n)
var $S = 8$
var $F = 2^{2^n} + 1$
repeat $2^{n-1} - 1$ times :
$S = (((S \times S) - 2) \times ((S \times S) - 2) - 2) \pmod F$
if $S = 0$ return PRIME else return COMPOSITE

Date: January 11 , 2012.

2.2. **Proof of correctness.** Let us define sequence S_i as :

$$S_i = \begin{cases} 8 & \text{if } i = 0; \\ (S_{i-1}^2 - 2)^2 - 2 & \text{otherwise .} \end{cases}$$

Theorem 2.1. *$F_n = 2^{2^n} + 1, (n \geq 2)$ is a prime if and only if F_n divides $S_{2^{n-1}-1}$.*

Proof. Let us define $\omega = 4 + \sqrt{15}$ and $\bar{\omega} = 4 - \sqrt{15}$ and then define L_n to be $\omega^{2^{2n}} + \bar{\omega}^{2^{2n}}$, we get $L_0 = \omega + \bar{\omega} = 8$, and
$L_{n+1} = \omega^{2^{2n+2}} + \bar{\omega}^{2^{2n+2}} = (\omega^{2^{2n+1}})^2 + (\bar{\omega}^{2^{2n+1}})^2 =$
$= (\omega^{2^{2n+1}} + \bar{\omega}^{2^{2n+1}})^2 - 2 \cdot \omega^{2^{2n+1}} \cdot \bar{\omega}^{2^{2n+1}} =$
$= ((\omega^{2^{2n}} + \bar{\omega}^{2^{2n}})^2 - 2 \cdot \omega^{2^{2n}} \cdot \bar{\omega}^{2^{2n}})^2 - 2 \cdot \omega^{2^{2n+1}} \cdot \bar{\omega}^{2^{2n+1}} =$
$= ((\omega^{2^{2n}} + \bar{\omega}^{2^{2n}})^2 - 2 \cdot (\omega \cdot \bar{\omega})^{2^{2n}})^2 - 2 \cdot (\omega \cdot \bar{\omega})^{2^{2n+1}}$
and since $\omega \cdot \bar{\omega} = 1$ we get :
$L_{n+1} = (L_n^2 - 2)^2 - 2$

Because the L_n satisfy the same inductive definition as the sequence S_i , the two sequences must be the same .

Proof of necessity :

If $2^{2^n} + 1$ is prime then $S_{2^{n-1}-1}$ is divisible by $2^{2^n} + 1$

We rely on simplification of the proof of Lucas-Lehmer test by Oystein J. R. Odseth , see [1].First notice that 3 is quadratic non-residue $\pmod{F_n}$ and that 5 is quadratic non-residue $\pmod{F_n}$. Euler's criterion then gives us :
$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ and $5^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$
On the other hand 2 is a quadratic-residue $\pmod{F_n}$, Euler's criterion gives:
$2^{\frac{F_n-1}{2}} \equiv 1 \pmod{F_n}$
Next define $\sigma = 2\sqrt{15}$, and define X as the multiplicative group of $\{a + b\sqrt{15} | a, b \in Z_{F_n}\}$ .We will use following lemmas :

Lemma 2.1. : $(x + y)^{F_n} = x^{F_n} + y^{F_n} \pmod{F_n}$
Lemma 2.2. : $a^{F_n} \equiv a \pmod{F_n}$ (Fermat little theorem)

Then in group X we have :

$(6 + \sigma)^{F_n} \equiv (6)^{F_n} + (\sigma)^{F_n} \pmod{F_n} =$
$= 6 + (2\sqrt{15})^{F_n} \pmod{F_n} =$

$= 6 + 2^{F_n} \cdot 15^{\frac{F_n-1}{2}} \cdot \sqrt{15} \pmod{F_n} =$
$= 6 + 2 \cdot 3^{\frac{F_n-1}{2}} \cdot 5^{\frac{F_n-1}{2}} \cdot \sqrt{15} \pmod{F_n} =$
$= 6 + 2 \cdot (-1) \cdot (-1) \cdot \sqrt{15} \pmod{F_n} =$
$= 6 + 2\sqrt{15} \pmod{F_n} = (6 + \sigma) \pmod{F_n}$

We chose σ such that $\omega = \frac{(6+\sigma)^2}{24}$. We can use this to compute $\omega^{\frac{F_n-1}{2}}$ in the group X :

$$\omega^{\frac{F_n-1}{2}} = \frac{(6+\sigma)^{F_n-1}}{24^{\frac{F_n-1}{2}}} = \frac{(6+\sigma)^{F_n}}{(6+\sigma)\cdot 24^{\frac{F_n-1}{2}}} \equiv \frac{(6+\sigma)}{(6+\sigma)\cdot(-1)} \pmod{F_n} = -1 \pmod{F_n}$$

where we use fact that :

$$24^{\frac{F_n-1}{2}} = (2^{\frac{F_n-1}{2}})^3 \cdot (3^{\frac{F_n-1}{2}}) \equiv (1^3) \cdot (-1) \pmod{F_n} = -1 \pmod{F_n}$$

So we have shown that :

$$\omega^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

If we write this as $\omega^{\frac{2^{2^n}+1-1}{2}} = \omega^{2^{2^n-1}} = \omega^{2^{2^n-2}} \cdot \omega^{2^{2^n-2}} \equiv -1 \pmod{F_n}$,multiply both sides by $\bar{\omega}^{2^{2^n-2}}$, and put both terms on the left hand side to write this as :
$\omega^{2^{2^n-2}} + \bar{\omega}^{2^{2^n-2}} \equiv 0 \pmod{F_n}$
$\omega^{2^{2(2^{n-1}-1)}} + \bar{\omega}^{2^{2(2^{n-1}-1)}} \equiv 0 \pmod{F_n} \Rightarrow S_{2^{n-1}-1} \equiv 0 \pmod{F_n}$

Since the left hand side is an integer this means therefore that $S_{2^{n-1}-1}$ must be divisible by $2^{2^n} + 1$.

Proof of sufficiency :

If $S_{2^{n-1}-1}$ is divisible by $2^{2^n} + 1$, then $2^{2^n} + 1$ is prime

We rely on simplification of the proof of Lucas-Lehmer test by J. W. Bruce , see [2].If $2^{2^n} + 1$ is not prime then it must be divisible by some prime factor F less than or equal to the square root of $2^{2^n} + 1$. From the hypothesis $S_{2^{n-1}-1}$ is divisible by $2^{2^n} + 1$ so $S_{2^{n-1}-1}$ is also multiple of F , so we can write :
$\omega^{2^{2(2^{n-1}-1)}} + \bar{\omega}^{2^{2(2^{n-1}-1)}} = K \cdot F$, for some integer K . We can write this equality as :
$\omega^{2^{2^n-2}} + \bar{\omega}^{2^{2^n-2}} = K \cdot F$
Note that $\omega \cdot \bar{\omega} = 1$ so we can multiply both sides by $\omega^{2^{2^n-2}}$ and rewrite

this relation as :
$\omega^{2^{2^n-1}} = K \cdot F \cdot \omega^{2^{2^n-2}} - 1$. If we square both sides we get :
$\omega^{2^{2^n}} = (K \cdot F \cdot \omega^{2^{2^n-2}} - 1)^2$
Now consider the set of numbers $a + b\sqrt{15}$ for integers a and b where $a + b\sqrt{15}$ and $c + d\sqrt{15}$ are considered equivalent if a and c differ by a multiple of F , and the same is true for b and d . There are F^2 of these numbers , and addition and multiplication can be verified to be well-defined on sets of equivalent numbers. Given the element ω (considered as representative of an equivalence class) , the associative law allows us to use exponential notation for repeated products : $\omega^n = \omega \cdot \omega \cdots \omega$, where the product contains n factors and the usual rules for exponents can be justified . Consider the sequence of elements $\omega, \omega^2, \omega^3...$. Because ω has the inverse $\bar{\omega}$ every element in this sequence has an inverse . So there can be at most $F^2 - 1$ different elements of this sequence. Thus there must be at least two different exponents where $\omega^j = \omega^k$ with $j < k \leq F^2$. Multiply j times by inverse of ω to get that $\omega^{k-j} = 1$ with $1 \leq k - j \leq F^2 - 1$.
So we have proven that ω satisfies $\omega^n = 1$ for some positive exponent n less than or equal to $F^2 - 1$. Define the order of ω to be smallest positive integer d such that $\omega^d = 1$. So if n is any other positive integer satisfying $\omega^n = 1$ then n must be multiple of d . Write $n = q \cdot d + r$ with $r < d$. Then if $r \neq 0$ we have $1 = \omega^n = \omega^{q \cdot d + r} = (\omega^d)^q \cdot \omega^r = 1^q \cdot \omega^r = \omega^r$ contradicting the minimality of d so $r = 0$ and n is multiple of d .
The relation $\omega^{2^{2^n}} = (K \cdot F \cdot \omega^{2^{2^n-2}} - 1)^2$ shows that $\omega^{2^{2^n}} \equiv 1 \pmod F$. So that 2^{2^n} must be multiple of the order of ω . But the relation $\omega^{2^{2^n-1}} = K \cdot F \cdot \omega^{2^{2^n-2}} - 1$ shows that $\omega^{2^{2^n-1}} \equiv -1 \pmod F$ so the order cannot be any proper factor of 2^{2^n} , therefore the order must be 2^{2^n} . Since this order is less than or equal to $F^2 - 1$ and F is less or equal to the square root of $2^{2^n}+1$ we have relation : $2^{2^n} \leq F^2 - 1 \leq 2^{2^n}$. This is true only if $2^{2^n} = F^2 - 1 \Rightarrow 2^{2^n} + 1 = F^2$. We will show that Fermat number cannot be square of prime factor .

Theorem 2.2. *Any prime divisor p of $F_n = 2^{2^n} + 1$ is of the form $k \cdot 2^{n+2} + 1$ whenever n is greater than one .*

Proof. For proof see [3]

□

So prime factor F must be of the form $k \cdot 2^{n+2} + 1$, therefore we can write :
$2^{2^n} + 1 = (k \cdot 2^{n+2} + 1)^2$
$2^{2^n} + 1 = k^2 \cdot 2^{2n+4} + 2 \cdot k \cdot 2^{n+2} + 1$

$2^{2^n} = k \cdot 2^{n+3} \cdot (k \cdot 2^{n+1} + 1)$

The last equality cannot be true since $k \cdot 2^{n+1} + 1$ is an odd number and 2^{2^n} has no odd prime factors so $2^{2^n} + 1 \neq F^2$ and therefore we have relation $2^{2^n} < F^2 - 1 < 2^{2^n}$ which is contradiction so therefore $2^{2^n} + 1$ must be prime .

$\square$

3. Acknowledgments

I wish to express my gratitude to Bojan Terzich for grammatical improvement of the text .

References

1. Proof of necessity by Oystein J. R. Odseth available at :
   http://en.wikipedia.org/wiki/Lucas-Lehmer_primality_test
2. Proof of sufficiency by J. W. Bruce available at :
   http://www.mersennewiki.org/index.php/Lucas-Lehmer_Test
3. Proof of Edouard Lucas theorem available at :
   http://en.wikipedia.org/wiki/Fermat_number

E-mail address: tersit26@gmail.com