In this note we discuss the basic properties of Mersenne and Fermat numbers. We are particularly interested in the primality of these numbers.

1. Fermat numbers.

In this section we discuss numbers of the form $2^m + 1$.

Lemma 1.1. *Let $m \geq 1$. If $2^m + 1$ is prime, then m is a power of 2.*

Proof. Suppose $m = ab$ with a odd. Let $q = 2^b + 1$. Then $2^b \equiv -1 \pmod{q}$ and hence $2^m = 2^{ab} \equiv (-1)^a = -1 \pmod{q}$. This means that q divides the prime number $2^m + 1$. Since $q > 1$, we must have $q = 2^m + 1$ and hence $b = m$. It follows that $a = 1$. Therefore the only odd divisor of m is $a = 1$. This means that m is a power of 2, as required.

Definition. For $k \geq 0$, the *k-th Fermat number* is defined as $F_k = 2^{2^k} + 1$.

Fermat already showed that F_k is prime for $k \leq 4$. For these values of k the numbers are 3, 5, 17, 257 and 65537. Euler showed that F_5 is divisible by 641 and is hence not prime. It is now known that F_k is not prime for $5 \leq k \leq 32$ and several other values of k. For $k \leq 11$ the numbers F_k have been completely factored.

Lemma 1.2. *Let $k \geq 2$ and let q be a prime divisor of $F_k = 2^{2^k} + 1$. Then we have $q \equiv 1 \pmod{2^{k+2}}$.*

Proof. Since q divides F_k, we have $2^{2^k} \equiv -1 \pmod{q}$. It follows that the order of the element 2 of the multiplicative group $(\mathbf{Z}/q\mathbf{Z})^*$ is 2^{k+1}. We observe that $(1 + 2^{2^{k-1}})^2 \equiv 2^{2^{k-1}+1} \pmod{F_k}$. Since $k \geq 2$, the exponent $2^{k-1} + 1$ is odd. It follows that 2 itself is also a square modulo F_k and hence modulo q. Since the order of $2 \in (\mathbf{Z}/q\mathbf{Z})^*$ is 2^{k+1}, the order of any of its square roots is 2^{k+2}. It divides the order of the group $(\mathbf{Z}/q\mathbf{Z})^*$ which is $q - 1$. This implies the lemma.

Proposition 1.3. *(Pépin 1877) Let $k \geq 1$. Then the Fermat number $F = F_k = 2^{2^k} + 1$ is prime if and only if $3^{(F-1)/2} \equiv -1 \pmod{F}$.*

Proof. Since $k \geq 1$, we have $F \equiv 5 \pmod{12}$ therefore 3 is not a square modulo 3. If F is prime, this implies that $3^{(F-1)/2} \equiv -1 \pmod{F}$. Conversely, let q be a prime divisor of F. If $3^{(F-1)/2} \equiv -1 \pmod{F}$, then we have the same congruence modulo q. The fact that $F - 1$ is a power of 2 implies then that the order of $3 \in (\mathbf{Z}/q\mathbf{Z})^*$ is $F - 1$. It follows that $F - 1$ divides $q - 1$, so that $F = q$ and hence F is prime.

Since $(F_k - 1)/2 = 2^{2^k - 1}$, one Pépin test consists of $2^k - 1$ squarings modulo $F_k = 2^{2^k} + 1$. The amount of work involved is proportional to 2^{3k}. This grows so rapidly with k that already for $k = 33$, performing the test involves too much computing time. When k is this large, proving that a Fermat number F_k is not prime is done by factoring it using factoring algorithms that find small prime factors quickly. The elliptic curve method is very suitable in this sense.

2. Mersenne numbers.

In this section we discuss numbers of the form $2^m - 1$.

Lemma 2.1. *Let $m \geq 1$. If $2^m - 1$ is prime, then m is a prime number.*

Proof. Suppose $m = ab$. Let $q = 2^b - 1$. Then $2^b \equiv 1 \pmod{q}$ and hence $2^m = 2^{ab} \equiv 1^a = 1 \pmod{q}$. This means that q divides the prime number $2^m + 1$. So either $q = 1$ in which case $b = 1$ or $q = 2^m - 1$, in which case $b = m$. It follows that m cannot be factored in a non-trivial way, so that it is prime.

Definition. For a prime number p, the *p-th Mersenne number* is defined as $M_p = 2^p - 1$.

Already Mersenne decided for several small primes p whether the number M_p is prime or not. The number M_{127} was the largest prime number known for over a century. Only in 1951 a larger prime number was found. Also today, the largest prime number known is a Mersenne prime. It is M_p with $p = 43112609$.

Lemma 2.2. *Let p be a prime and let q be a prime divisor of $M_p = 2^p - 1$. Then we have $q \equiv 1 \pmod{p}$.*

Proof. Since q divides M_p, we have $2^p \equiv 1 \pmod{q}$. It follows that the order of the element 2 of the multiplicative group $(\mathbf{Z}/q\mathbf{Z})^*$ is p. Therefore p divides the order of the group $(\mathbf{Z}/q\mathbf{Z})^*$ which is $q - 1$. This implies the lemma.

Proposition 2.3. *(Lucas 1878–Lehmer 1930's). Let $p > 3$ be a prime and let $M = 2^p - 1$. Let $2+\sqrt{3}$ denote the image of X in the ring $R = (\mathbf{Z}/M\mathbf{Z})[X]/(X^2-3)$. Then the Mersenne number M is prime if and only if $(2 + \sqrt{3})^{(M+1)/2} = -1$ in R.*

Proof. Since $p > 3$ we have $M \equiv 7 \pmod{12}$. Therefore, if M is prime, 3 is a non-square modulo M and R is a finite field of M^2 elements. From the identity $(1+\sqrt{3})^2 = 2(2+\sqrt{3})$, we deduce

$$(2 + \sqrt{3})^{(M+1)/2} \;=\; (1 + \sqrt{3})^{M+1} 2^{-(M-1)/2} 2^{-1}.$$

Since $M \equiv -1 \pmod{8}$, the number 2 is a square modulo M and we have $2^{(M-1)/2} = 1$ in R. In addition we have $(1+\sqrt{3})^{M+1} = (1+\sqrt{3})(1-\sqrt{3}) = -2$ in R. Substituting these two identities gives

$$(2 + \sqrt{3})^{(M+1)/2} \;=\; -2 \cdot 1 \cdot 2^{-1} \;=\; -1,$$

as required.

Conversely, let q be a prime divisor of M. Since $M + 1$ is a power of 2, the fact that $(2 + \sqrt{3})^{(M+1)/2} = -1$ implies that the element $2 + \sqrt{3}$ has order $M + 1$ in R^* and hence in the group $(\mathbf{Z}/q\mathbf{Z})[X]/(X^2 - 3)^*$. It follows that $M + 1 < q^2$ and hence $M = q$ so that M is prime.

Corollary 2.4. *Let p be a prime and let s_k be the sequence that is recursively defined by $s_0 = 4$ and $s_{k+1} = s_k^2 - 2$ for $k \geq 0$. Then $M = 2^p - 1$ is prime if and only if $s_{p-2} \equiv 0 \pmod{M}$*

Proof. Let R be the ring of Proposition 2.3. We define $a_k, b_k \in \mathbf{Z}/M\mathbf{Z}$ by putting $a_k + b_k\sqrt{3} = (2 + \sqrt{3})^{2^k}$ for $k \geq 0$. We have that $a_{k+1} = a_k^2 - 3b_k^2$ for $k \geq 0$. Since

$a_k^2 - 3b_k^2 = 1$, this means that $a_{k+1} = 2a_k^2 - 1$ for $k \geq 0$. We claim that $(2+\sqrt{3})^{(M+1)/2} = -1$ in R if and only if $a_{p-2} \equiv 0 \pmod{M}$. Indeed, we have $(2+\sqrt{3})^{(M+1)/2} = -1$ if and only if $a_{p-1} = -1$ and $b_{p-1} = 0$. By the recurrence relation above this is equivalent to $a_{p-2} = 0$.

Proposition 3.3 implies then that M is prime if and only if $a_{p-2} =$ in $\mathbf{Z}/M\mathbf{Z}$. Since the sequences s_k and $2a_k$ satisfy the same recurrence relations, we have $s_k = 2a_k$ for all $k \geq 0$. This implies the corollary.

Since $(M_p + 1)/2 = 2^{p-1}$, one Lucas-Lehmer test consists of $p - 1$ squarings modulo $M_p = 2^p - 1$. The amount of work involved is proportional to p^3. Nowadays, the test is used in practice to search for large Mersenne prime numbers.